Avrupa Birliği Çerçevesinde Kişisel Verilerin Korunması

Prof. Dr. Vesile Sonay Evik*

I- Genel Olarak

1970'li yıllardan itibaren bilişim teknolojilerinin gelişmeye başlaması ile bireylere ait verilerin kaydedilmesi, saklanması ve başkalarına aktarılması kolaylaşması üzerine kişisel verilerin korunması ihtiyacı ortaya çıkmıştır. Kişisel verilen korunmasına ilişkin ilk yasal düzenlemeler, 1970 yılında Almanya'da (Hessen Federe Devletinde), 1973'te İsveç'te, 1976'da Almanya Federal Kanun olarak, Danimarka, Norveç ve Fransa'da 1978 yılında yapılmıştır; sonraki yıllarda bunları Lüksemburg, Belçika, İspanya ve Portekiz takip etmiştir. Söz konusu yasal düzenlemelerle devletler özellikle kendi vatandaşlarına ait verilerin, kendi sınırlarından çıkarılarak uluslararası dolaşımını kontrol altına almaya çalışmışlardır[1]. Bu yasal düzenlemelerin uluslararası veri akışını, dolayısıyla ticareti kısıtlayacağını dikkate alan OECD[2], Avrupa Konseyi[3], Birleşmiş Milletler[4] gibi bazı uluslararası kuruluşlar da kişisel verilerin korunması açısından devletlerin hepsinin üzerinde uzlaşabileceği asgari koruma standartlarını, kişisel verilerin hukuka uygun elde edilmesi, amacına uygun işlenmesi, amaçla sınırlı olarak saklanması, ilgili kişi tarafından kişisel erişim, ayrımcılık yapılmaması, güvenlik önlemlerinin alınması, ihlal durumunda sorumluluk taşınması gibi rehber ilkeleri belirlemeye çalışmışlardır[5].

Kişisel verilerin teknoloji ve ekonomik ticari ilişkilerin gelişimiyle birlikte Avrupa Birliği nezdinde de temel bir insan hakkı olarak korunması ihtiyacı konusunda bilinçlenme oluşmuştur. 1990'lı yıllarda ilk kez bu konuda çalışmalara başlayan AB, bu konuda ilk düzenlemesini "Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Açısından Bireylerin Korunmasına İlişkim Avrupa Parlamentosu ve Avrupa Konseyi Yönergesi" şeklinde 24 Ekim 1995'te yayınlamıştır. Yönerge ile hem birlik ülkelerine kişisel verilerin korunmasına ilişkin yüksek standartlar getirilirken hem de elektronik ticaretin ekonomide çok daha büyük bir yer kaplaması sebebiyle birlik ülkeleri içinde verilerin serbest dolaşıma ilişkin düzenlemeler yapılmıştır.[6]

7 Aralık 2000 tarihinde imzalanan Avrupa Birliği Temel Haklar Şartının (daha sonra 1 Aralık 2009'da imzalanan Lizbon Antlaşması ile bağlayıcılık kazanan) 8. Maddesinde kişisel verilerin korunması ayrı bir başlık altında temel bir insan hakkı olarak düzenlenmiştir. Buna göre herkes kendisine ilişkin kişisel bilgilerinin korunmasını isteme hakkına sahiptir. Bu veriler belirli amaçlarla ve ilgili kişinin rızasına veya kanunda öngörülen başka bir yasal temele dayanarak dürüstlük kuralına uygun olarak işlenmelidir. Herkes kendisi ile ilgili olarak toplanmış verilere erişme ve bunların düzeltilmesini sağlama hakkına sahiptir. Bu kurallara uyulması, bağımsız bir makamın denetimine tabidir. Ayrıca 95/46/EC sayılı Yönerge esas alınarak sektörel bazlı bazı düzenlemeler de kabul edilmiştir. Örneğin elektronik haberleşme sektöründeki eksiklikleri

---

*Galatasaray Üniversitesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı Öğretim Üyesi.

[1] Develioğlu Hüseyin Murat, 6698 Sayılı, Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, Oniki Levha, İstanbul, 2017, 6.

[2] 23.9.1980 tarihinde kabul edilen ve 2013 yılında güncellenen Kişisel Alanın Korunmasına ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler, tavsiye niteliğinde olup, amacı serbest piyasa ekonomisinde verilerin serbest dolaşımını sağlamak, veri sahiplerinin menfaatlerini korumak ve sınır ötesi kişisel veri akışının engellenmesine neden olabilecek durumları ortadan kaldırmaktır. Develioğlu, 6. Uyarer, 43.

[3] 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulmasında Kişilerin Korunmasına İlişkin Avrupa Sözleşmesi 1981 yılında imzaya açılmış olup, Türkiye tarafından 2016 tarihinde onaylanmıştır. Uyarer, 48.

[4] 1990 yılında 45/95 Sayılı Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler de tavsiye niteliğinde olup, üye ülke mevzuatlarında yer alması gereken asgari standartları belirlemiştir. Develioğlu, 10.

[5] Develioğlu, 5 vd.; Uyarer, 43-49.

[6] Paul M. Schwartz, "European Data Protection Law and Restrictions on International Data Flows", 80 Iowa Law Review, 471, 1994, 483. Ayrıca bkz. Hayrunnisa Özdemir, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Ankara, Seçkin Yayınları, 2009'dan aktaran Ayözger Çiğdem, Kişisel Verilerin Korunması-Elektronik Haberleşme sektörüne İlişkin Özel Düzenlemeler, Be ta, İstanbul, 2016, 74.

kapatmak ve bu alandaki boşluğu doldurmak için 1997 /66/EC sayılı Yönerge, 2002/58/EC sayılı Elektronik Veri Koruma Yönergesi (Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Özel Hayatın Gizliliğinin Korunmasına İlişkin Yönerge), 2006/24(EC sayılı Avrupa Birliği Veri Saklama Direktifi (Halka Açık İletişim Hizmetleri veya İletişim Ağlarına İlişkin Olarak Üretilen veya İşlenen Verilerin Saklanmasına İlişkin Yönerge), 2009/136/EC sayılı Avrupa Birliği Vatandaşlık Hakkı Yönergesi bu kapsamdadır. Teknolojik gelişmeler ve globalleşmenin getirdiği ekonomik ve sosyal sorunlar ve Avrupa Birliği Adalet Divanının kararlarının mevcut direktifin yetersiz kaldığını, birlik ülkelerinde farklı düzenlemeler nedeniyle farklı uygulamaların olduğunu gözler önüne sermesiyle, artık daha ayrıntılı, ihtiyaçlara cevap verebilecek birliğe üye ülkeler arasında yeknesak bir yeni bir düzenleme yapılması için çalışmalar yapılmıştır. Bunun sonucunda Avrupa Parlamentosu tarafından 2016/679 Sayılı 27 Nisan 2016 tarihinde kabul edilen Avrupa Birliği Genel Veri Koruma Tüzüğü 24 Mayıs 2018 tarihinde yürürlüğe girmiş ve 1995 tarihli (95/46/EC) yönergeyi ilga etmiştir. Hemen ardından da 2016/680 sayılı Kişisel Verilerin Ceza Adaleti ve Polis İşbirliği Alanında Kullanılmasına Yönelik Gerçek Kişilere Ait Kişisel Verilerin Yetkili Otoriteler Tarafından Suçların Önlenmesi, Soruşturulması ve Tespit Edilmesi veya Cezaların İnfazı Amacıyla İşlenmesi ve Bu Nevi Kişisel Verilerin Serbest Dolaşımı Hakkında Yönerge, 27 Nisan 2016 tarihinde kabul edilmiştir[7]. Tüzük verilerin işlenmesine uygulanabilecek genel kuralları içerirken, yönerge adli uygulamalarda verilerin işlenmesine uygulanacak özel nitelikte kuralları içermektedir. Bu nedenle de kapsamı suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezai yaptırımların uygulanması amacıyla yetkili makamlar tarafından kişisel verilerin işlenmesi ile sınırlıdır[8].

II-Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Açısından Bireylerin Korunmasına İlişkim Avrupa Parlamentosu ve Avrupa Konseyi Yönergesi

Kişisel verilerin korunması açısından ilk düzenleme 24.10.1995 tarihinde yürürlüğe giren 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Açısından Bireylerin Korunmasına İlişkim Avrupa Parlamentosu ve Avrupa Konseyi Yönergesi'dir. 34 maddeden oluşan yönergenin 1. Maddesinde birlik ülkeleri ilk kez özel hayatın korunması hakkı kapsamında bireylerin kişisel verilerini korumakla yükümlü tutulmuşlardır. Ayrıca birlik ülkelerinin üye ülkeler arasındaki veri dolaşımını engellemeyecekleri ve yasaklamayacakları öngörülmüştür. Böylece kişisel verilerin korunması ile bu verilere ulaşım arasındaki denge de korunmak istenmiştir[9].

Yönergede kişisel verilerin korunması açısından temel kavramlar ve ilkeler belirlenmekle birlikte, etkili bir koruma sağlamak adına, yönergenin uygulanmasını gözetmek üzere her bir üye devlet tarafından en az bir ulusal denetim makamı oluşturulması öngörülmüştür. Ayrıca yönergenin uygulanmasını ve gelişimini sağlamak için "Madde 29 Çalışma Grubu" kurulmuştur. Bu çalışma grubu, üye devletlerde yönergenin uygulanmasını gözetmek ve üye devletler ile Avrupa Birliği Komisyonuna kişisel verilen korunması konusunda tavsiyelerde bulunmak yönergenin üye devletler tarafından yeknesak şekilde uygulanmasını denetlemekle de görevlendirilmiştir[10]

Yönergenin uygulanması, birliğe üye devletlerin yönergedeki düzenlemeleri kendi iç hukuklarına aktarmaları ile mümkün olabilmektedir Yönergede belirlenen temel prensiplere dayanarak her bir üye devlette kişisel verilen korunmasına dair düzenlemeler yapılmaya başlanmıştır. Ancak yönergenin doğrudan uygulanabilen özelliği olmadığı için her üye devlette farklı yasal düzenleme yapılması ile birlik içinde yeknesak bir uygulama sağlanamamıştır. Bu

---

[7] https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L0680&from=it

[8] Bozbayındır Bostancı Gülşah, "Avrupa Birliği Ceza Hukuku'nda Polis ve Ceza Adaleti Otoritelerine Yönelik 2018/680 Sayılı Direktif: Kişisel Verilerin Ceza Adalet Mekanizmalarında Korunmasına Getirilen Standartlar ve Direktife Yönelik Eleştiriler", Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, 2018/2, 71.

[9] Uyarer Göçmen Sinem, Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Seçkin, Ankara, 2019, 57-58.

[10] Develioğlu, 11.

arada hızla gerçekleşen teknolojik gelişmeler ve küreselleşme, kişisel verilerin korunması açısından daha etkili, ayrıntılı, yeknesak, eşdeğer ve doğrudan uygulanabilir bir düzenlemeye ihtiyaç olduğu gerçeğini ortaya koymuştur[11]. Yönerge pek çok eksikliğine rağmen kişisel verilerin korunması açısından kendisinden sonra gelen pek çok ulusal ve uluslararası düzenlemeye kaynaklık etmiştir.

III- Avrupa Birliği Genel Veri Koruma Tüzüğü (General Data Protection Regulation (GDPR)

2010 Kasım ayında Avrupa Birliği Komisyonu tarafından "Avrupa Birliğinde Kişisel Veri Korunmasına İlişkin Kapsamlı Bir Yaklaşım" adında açıklama ile, 95/46/EC sayılı yönergenin hızlı teknolojik gelişmeler ve küreselleşme nedeniyle kişisel verilerin korunması açısından güncel ihtiyaçları karşılayamadığı gözden geçirilmesi gerektiği ifade edilmiştir[12]. Bu açıklamanın ardından başlayan yoğun çalışmalardan sonra 22.06.2011 tarihinde Avrupa Veri Koruma Denetmeni, Konseye mütalaasını sunmuş ve 25 Ocak 2012 tarihinde de Konsey tarafından teklif edilen metin, 07.03.2012 tarihinde Avrupa Veri Koruma Denetmeni tarafından kabul edilmiştir. Mevcut metin üzerinde yapılan çalışmalar neticesinde 15.12.2015 tarihinde "Avrupa Birliği Genel Veri Koruma Tüzüğü" şeklinde hazırlanan metin Avrupa Parlamentosu, Avrupa Konseyi ve Avrupa Komisyonu tarafından anlaşmaya varılmış; 2016/679 sayı ile 27 Nisan 2016 tarihinde Avrupa Parlamentosu tarafından kabul edilerek; 25.Mayıs 2018 tarihinde yürürlüğe girmiştir[13].

Tüzüğün amacı, birlik ülkeleri arasında ve bu ülkelerden, birlik üyesi olmayan ülkelere veya uluslararası organizasyonlara veri transferini düzenlemek, veri güvenliği konusunda birlik oluşturarak veri korumasında tüm ülkelerde eşdeğer bir koruma sağlamak ve bu sayede veri sahiplerinin verilerinin korunduğuna ilişkin güvenlerini arttırarak elektronik ticaretin ve ekonominin gelişmesini sağlamaktır.[14]

95/46/EC sayılı Yönergede kişisel veri "belirli ya da kimliği belirlenebilir gerçek kişi ile ilişkilendirilebilen her türlü bilgi", "bir kişinin doğrudan veya dolaylı olarak tanımlanabilmesine imkân sağlayan kişinin kimlik numarası, fiziksel, psikolojik, duygusal, ekonomik ve kültürel kimliği veya sosyal kimliği" olarak ifade edilmişti. Avrupa Birliği Veri Koruma Tüzüğünde ise kişisel veri "belirli veya belirlenebilir bir gerçek kişiye ilişkin her türlü bilgidir; belirlenebilir gerçek kişi bir tanımlayıcıya, örneğin ismine, kimlik numarasına, konum bilgisine, bir çevrimiçi tanımlayıcıya ya da kişinin fiziksel fizyolojik, genetik, ruhsal, ekonomik, kültürel veya sosyal kimliğine ilişkin bir veya birden fazla faktöre atıfta bulunularak doğrudan veya dolaylı olarak belirlenebilen bir kişidir" şeklinde tanımlanmıştır.

Tüzük yönergedeki kişisel veri tanımını genişletilerek, IP adresi, parmak izi alma, retina taraması gibi yollarla elde edilen kişilerin biyolojik verileri, konum bilgisi, kişilerin fiziksel, psikolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliği gibi verilerin tamamı kişisel veri olarak kabul edilmiştir.[15]

Kişisel verilerin korunması açısından getirilen yeni düzenlemenin şüphesiz en önemli özelliği, doğrudan uygulanabilir düzenleme olmayan "yönerge" yerine doğrudan uygulanabilir düzenleme olan "tüzük" olması; dolayısıyla üye devletler arasında yeknesak bir uygulamayı sağlamış bulunmasıdır[16].

---

[11] Avrupa Komisyonu'nun 2010 Kasım ayında "Avrupa Birliğinde Kişisel Veri Korunmasına Kapsamlı Bir Yaklaşım" açıklaması ile bu konuda korumanın güçlendirilmesine gerektiği dile getirilmiştir. Açıklamanın ardından yapılan çalışmalar sonucunda Avrupa Birliği Genel Koruma Tüzüğü hazırlanmıştır. Develioğlu, 12.

[12] Develioğlu, 12.

[13] 04.05.2016 tarihli AB Resmi Gazetesinde yayınlanarak 25 Mayıs 2018 tarihinde yürürlüğe girmiştir.

[14] Avrupa Birliği Genel Veri Koruma Tüzüğü için bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN; https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679&from=IT.

[15] https://www.kefron.com/blog/will-term-personal-data-defined-within-gdpr; Uyarer, 67.

[16] Develioğlu, 12.

Tüzüğün ikinci en önemli özelliği, tüzüğün uygulanma alanının genişliği itibariyle tüm dünya ülkelerinde uygulanabilir olmasıdır. Şöyle ki, tüzüğün yer açısından uygulanma alanına ilişkin 3. maddesinde veri işlemenin Avrupa Birliği sınırları içinde olup olmadığına bakılmaksızın, Avrupa Birliğindeki bir veri sorumlusu veya veri işleyene ait bir işletmenin faaliyeti kapsamında gerçekleşmesi gerekir. Buradaki işletme kavramının, Avrupa Adalet Divanı tarafından çok geniş olarak kabul gördüğünü belirtmekte yarar vardır[17]. Ayrıca Tüzüğün maddesinin 2. Fıkrası uyarınca AB'de bulunmasa dahi, veri sorumlusu veya veri işleyenin işleme faaliyetinin (ilgili kişinin ödeme yapıp yapmadığına bakılmaksızın) AB'de bulunan ilgili kişilere mal ve hizmet sunulmasına ilişkin olması halinde de tüzük uygulama alanı bulabilecektir. Tüzüğün uygulanması AB'de bulunan ilgili kişilerin yine AB sınırları içindeki davranışlarının gözlenmesine ilişkin işleme faaliyetlerinin varlığında da söz konusudur. Böylece AB'de bulunmayan veri sorumlusu ve veri işleyene karşı tüzükten doğan haklarını korumak için AB'ye üye ülkedeki yetkili denetim makamına başvurması mümkündür[18].

AB'de bulunmayan veri sorumlusu veya veri işleyeni tarafından AB'de bulunan kişilere mal ve hizmet sunulması halinde tüzük uygulanacaktır. Ancak bunun için, AB'de bulunan müşterilerin veya kullanıcıların hedef alınarak, örneğin üye devletlerden biri veya bir kaçında kullanılan bir dilde mal veya hizmet sunulması gerekmektedir. Salt veri sorumlusuna veya veri işleyene ait bir internet sitesine, e-posta adresine veya diğer iletişim bilgilerine Avrupa Birliğinden ulaşılabilmesi AB'de bulunan ilgili kişilere mal ve hizmet sunulması olarak kabul edilemeyecektir. Örneğin bir Türk şirketinin internet sitesine Almanya'da satmak üzere Türkçe ve Türk Lirası ile verdiği ilanlara AB'ne üye bir ülkeden ulaşılabilir olması tüzüğün uygulanmasını gerektirmemektedir. Ancak aynı şirketin internet sitesine Almanya'daki kişilere yönelik olarak Almanca dilinde ve Euro para biriminde mal satımına ilişkin ilanlar koyması durumunda tüzük uygulama alanı bulabilecektir. AB'de bulunan kişilerin davranışlarının gözlenmesine ilişkin işleme faaliyetleri de örneğin Türkiye'deki otelleri tanıtan Türk şirkete ait mobil telefon uygulamasının reklam göndermek amacıyla AB'de yer alan kişilerin konaklama konusundaki tercihlerini gözlemlemesi tüzüğün uygulanma alanı kapsamındadır[19]. Kişisel verilerin işlenmesinin Avrupa Birliği ülkeleri sınırları içinde yapılıp yapılmadığına bakılmaksızın, özellikle ekonomik ve ticari ilişkiler kapsamında Avrupa Birliğindeki bir veri sorumlusu veya veri işleyene ait bir işletmenin faaliyeti kapsamında gerçekleşmesi veya AB vatandaşlarına ilişkin olması halinde Avrupa Birliği dışındaki ülkelerde de tüzüğün getirdiği korumalardan yararlanabilecek olması, şüphesiz tüzüğün en önemli kazanımıdır[20].

Tüzüğün kişisel verilerin korunması açısından benimsediği temel prensipler de önceki düzenlemelere göre çok daha güvencelidir. Öncelikle kişisel verilerin hukuka hakkaniyete uygun olarak ve ilgili kişiyle bağlantılı olarak şeffaf şekilde işlenmesi gerektiği kabul edilmiştir (hukuka uygunluk, hakkaniyet ve şeffaflık prensipleri). Özellikle şeffaflık ilkesinin tüzüğe eklenmiş olması çok önemli bir gelişme olarak değerlendirilmektedir[21]. Kişisel veriler belirli, açık ve meşru amaçlar için toplanmalı ve bu amaçlara uygun olmayacak şekilde işlenmemelidir (amaçla sınırlı olma prensibi). Yeterli, ilgili ve işlendikleri amaçlarla bağlantılı olarak gerekli şekilde sınırlı olarak işlenmelidir (veri minimizasyonu prensibi). Veri doğru, gereken hallerde, güncel şekilde bulundurulmalıdır (doğruluk prensibi). Veriler işlendikleri amacın gerektirdiği süreyi aşmayacak şekilde ilgili kişinin belirlemesine izin veren bir halde tutulmalıdır. Ancak kamu yararı, bilimsel tarihi araştırma amacıyla veya istatiksel amaçlarla koruma için uygun teknik ve organizasyonel tedbirlerin alınması şartıyla daha uzun süre saklanabilir (sınırlı süre saklama prensibi). Ayrıca kişisel verilerin uygun ortam sağlanarak işlenmesi, yetkisiz ve hukuka aykırı şekilde işlenmelerine ve kazaen kaybolmalarına, imha edilmelerine veya hasara uğramalarına karşı güvenlik

[17] Avrupa Adalet Divanı'nın C230/14 sayılı davada 1.10.2015 tarihli kararında AB'de temsilcisi, iletişim adresi ve banka hesabı bulunmasını dikkate alarak işletmenin varlığı için "gerçek ve etkin bir faaliyetin" yeterli olduğunu belirtmiştir. Develioğlu, 16-17

[18] Hatta Tüzüğün 79. Maddesine göre AB'deki üye ülkenin mahkemesine başvurması da mümkündür.

[19] Develioğlu, 18-19.

[20] Dülger Volkan, Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi, İstanbul, 2019, 67.

[21] Opinion of the European Data Protection Supervisor on the Data Protection Reform Package, Par 114'dan Develioğlu, 45.

tedbirlerinin alınması gerekmektedir (bütünlük ve gizlilik prensibi). Veri sorumlusunun belirtilen ilkeler kapsamında sorumlu olduğu kabul edilmekle birlikte; onun bu ilkelere uygun hareket ettiğini ortaya koyabilmesi gerektiği de öngörülmüştür (sorumluluk prensibi).

Tüzükte, veri işleme süreçleri için veri sorumlusu ve veri işleyeni şeklinde tanımlanan sorumlu pozisyonların durumu daha ayrıntılı düzenlenmiştir. Veri sorumlusu, kişisel veri işleme sürecindeki amaçlara ve araçlara tek başına veya başkalarıyla birlikte karar veren gerçek veya tüzel kişi, kamu makamı veya kamu kurumu ya da diğer bir kamu kuruluşudur. Veri işleyeni ise veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi, kamu makamı veya kamu kurumu ya da diğer bir kamu kuruluşudur.

Tüzüğün getirdiği bir diğer önemli yenilik, kişilere kişisel verileri açısından daha fazla hak tanıması ve veri sorumlularının ve veri işleyenlerinin sorumluluğunu da artırmış olmasıdır. Veri sahiplerine, tanıdığı haklardan biri, bilgilendirilme hakkıdır. Kişinin kendisine ait verilerin işlendiğini bilmesi, haklarını kullanabilmesi açısından önemlidir. Bilinmeyen bir hakkın kullanılması mümkün olmayabilir. Veri sorumlusunun ilgili kişiyi aydınlatma yükümlülüğünün kapsamı, veriyi ilgili kişiden elde edip etmediğine göre değişmektedir (Tüzüğün 13 ve 14. Maddeleri). Veri sorumlusu, verinin işlenmesi sonrasında iletişim bilgilerini, verilerin hangi amaçla işlendiğini, hangi veri kategorilerinin işlendiğini, verilerin saklanma süresini, verilerin kimlere aktarılacağı gibi bilgileri vermekle yükümlüdür. Bu sayede tüzükte veri sahibine tanınan bir diğer haklar kullanılabilir hale gelmektedir. Tüzükte öngörülen, verilerin işlenmesinde şeffaflık ilkesinin sonucu olarak, veri sahibine tanınan ikinci hak, erişim hakkıdır. 15. Maddede ilgili kişinin veri sorumlusundan kişisel verilerinin işlenip işlenmediğine ilişkin bilgi isteyebileceği; işleniyorsa kendisinin kişisel verilerine ve maddede öngörülen bilgilerine erişmeyi talep edebileceği düzenlenmiştir. İlgili kişi istediğinde kendisine işlenmiş olan kişisel verilerinin kopyası verilmek zorundadır. Ancak kopya elde etme hakkı, başkalarının hak ve özgürlüklerini olumsuz şekilde etkilememelidir. Tüzüğün kişisel verilerin korunması açısından kabul ettiği doğruluk prensibi gereğince kişisel verilerin doğru olması gerekir. Bu ilkenin sonucu olarak, ilgili kişiye düzeltme hakkı da tanınmıştır. Tüzüğün 16. Maddesi uyarınca ilgili kişi, kişisel verilerinin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme hakkına sahiptir. Tüzükte yer alan en önemli hak, şüphesiz kişisel verilerinin silinmesini isteme bir diğer deyişle unutulma hakkıdır. Özellikle 2015 yılında Avrupa Adalet Divanının Google İspanya v. Mario Costeja Gonzales kararının etkisiyle tüzükte kişisel verilerinin silinmesini isteme hakkı, yönergeye kıyasla çok daha ayrıntılı şekilde düzenlenmiştir. Tüzüğün taslak aşamasındayken unutulma hakkı şeklinde ifade edilen bu hak, daha sonradan silinmesini isteme hakkı olarak düzenlenmiştir. Bu şekilde düzenlenmiş olması esasen yerinde olmuştur. Zira veri sorumlusuna edilgen bir yükümlülük yükleyen unutulma hakkına kıyasla, silinmesini isteme hakkının, etkin bir yükümlülük yüklemektedir[22]. Tüzüğün 17/1 maddesine göre ilgili kişi, kişisel verisinin silinmesini istediğinde veri sorumlusu, kişisel verinin gecikmeden silinmesini sağlamakla yükümlü tutulmuştur. Tüzükle tanınan bir diğer hak ise, ilgili kişinin belirli hallerde veri sorumlusundan işlemenin sınırlandırılmasını isteme hakkıdır. Örneğin ilgili kişi verinin doğruluğuna itiraz ederse veri sorumlusunun kişisel verinin doğruluğunu teyit etmesine elverişli bir süre için işlemeyi sınırlandırması gerekir (Tüzük 18. Madde). Ayrıca 19. Maddesine göre, veri sorumlusu, verinin yayıldığı diğer veri sorumlularının da aynı şekilde davranmalarını sağlaması için harekete geçmesi de gerekmektedir. Buna göre veri sorumlusu, verinin aktarıldığı her bir kişiye imkansız olmadıkça veya orantısız bir çaba gerektirmedikçe, verilerin düzeltilmesi, işlemenin sınırlandırılması, silinmesi gereğinden haber vermelidir. Ayrıca veri sorumlusu, ilgili kişinin talebi üzerine verinin aktarıldığı kişiler hakkında bilgilendirmekle de yükümlü tutulmuştur. Veri sahibi açısından böylelikle bildirimde bulunulmasını talep etme hakkı tanınmıştır[23]. Tüzüğün 20. Maddesine göre veri sahibi ayrıca veri sorumlusuna sağladığı kişisel verilerini genel olarak kullanılan ve bilişim sistemi tarafından okunabilen formatta talep etme ve başka bir veri sorumlusuna aktarma hakkına sahiptir. Ancak veri taşınabilirliği hakkı başkalarının hak ve özgürlüklerini olumsuz şekilde etkileyecek şekilde kullanılamaz. Tüzüğün 25. Maddesi ile,

[22] Ayözger; 41; Uyarer, 72.
[23] Develioğlu, 95.

ilk kez hukuki güvence altına alınan tasarımdan itibaren verinin korunması ilkesi de veri sahibi açısından tanınan önemli bir hak olarak kabul edilmek gerekir. Buna göre veri sorumlusu tasarımdan itibaren verinin korunması için gerekli tüm teknik ve organizasyonel tedbirleri almakla yükümlü tutulmuştur. Tüzüğün getirdiği bir başka önemli güvence, veri sorumlusu ve veri işleyeninin çeşitli hallerde veri koruma görevlisi ataması zorunluluğunun getirilmiş olmasıdır. Tüzüğün 37. Maddesine göre işleme, mahkemeler hariç, bir kamu kurumu ve kuruluşu tarafından gerçekleştiriliyorsa; veri sorumlusu ve işleyenin esas faaliyetleri tabiatı ve amaçları gereği ilgili kişilerin düzenli ve sistematik şekilde geniş çaplı olarak gözlemlemesiyle ilgili ise; esas faaliyetleri özel veri kategorilerinin veya cezai hükümler ve suçlara ilişkin kişisel verilerin geniş çapta işlenmesine ilişkinse veri koruma görevlisi atamalıdır. Atanan veri koruma görevlisinin kişisel verilerin korunması ve uygulanması konusunda uzmanlık bilgisi başta olmak üzere mesleki yetileri ve kendisine verilen görevlerine yerine getirme yetisi dikkate alınarak tayin edilir. Veri sorumlusu ve işleyeni söz konusu kişilerin görevlerini yerine getirirken bir menfaat çatışmasına neden olmadığını temin etmelidir. Bu kişiler veri sorumlusu veya işleyenin çalışanı olabileceği gibi hizmet sözleşmesi kapsamında görevlendirilebilir.

Tüzüğün getirdiği bir başka önemli yenilik, kişisel verinin hukuka uygun şekilde işlenebilmesi için veri sahibinden alınması gereken rızanın geçerlilik şartlarının kuvvetlendirilmiş olmasıdır[24]. Tüzüğün 4/11 maddesine göre rıza bir beyan ve aktif olumlu eylen şeklinde kendisiyle ilgili kişisel verilerin işlenmesine rıza gösterdiğini ortaya koyan, ilgili kişinin isteklerinin özgürce verilmiş, konuya özel, bilgilendirilmiş ve belirsizlik içermeyen bir ifadesidir. Böylece ilgili kişinin sessiz kalmasından örneğin kişisel verilerinin toplanmasına imkan veren ayarlarını değiştirmemesinden zımnen rıza gösterdiği sonucuna varılamayacağı; aktif bir eylem ile rızasını ortaya koyması gerektiği öngörülmüştür. Tüzüğün giriş kısmında verilen örnekte belirtildiği üzere bir internet sitesinde yer alan bir kutucuğun tıklanması, internetten bir hizmet satın almak için gereken teknik ayarların seçilmesi rızayı ortaya koyarken; önceden işaretlenmiş bir kutudaki işaretin silinmemesi gibi pasif, ihmali davranışlar rıza olarak nitelendirilemez[25]. Rızanın geçerli olması için rızanın hangi işleme faaliyetine ilişkin olduğu açıkça anlaşılabilir ve kolayca erişilebilir olmalıdır. Rıza özgür iradeyle verilmiş olmalıdır. Rızanın serbestçe verilip verilmediği değerlendirilmelidir. Özellikle bir hizmetin sunulmasına ilişkin sözleşmeler dahil olmak üzere, sözleşmenin ifası için gerekli olmayan bir işlemenin gerçekleştirilmesi şartına bağlanıp bağlanmadığına azami önem verilmelidir. Ayrıca ilgili kişi her zaman rızasını geri alabilme hakkına sahiptir. Rıza geri alınması, önceki işlemelerin hukuka uygunluğu etkilemeyecektir. Ancak bu konuda ilgili kişi rıza vermeden önce bilgilendirilmelidir. Rızanın geri alınması, verilmesi kadar kolay olmalıdır. Tüzüğün 8. Maddesinde çocukların kişisel verilerinin işlenmesi konusunda rızasının geçerliliği özel olarak düzenlenmiştir. Buna göre uzaktan ve elektronik araçlarla ve hizmet alıcısının bireysel talebi sonunda kural olarak ücret karşılığında sağlanan hizmetlerin sunulmasıyla ilgili olarak çocuğun kişisel verilerin işlenmesi konusundaki rızasının geçerliliği için en az 16 yaşında olması gerekir. 16 yaşın altındaki çocuklar açısından ancak velisinin rızası, yetkilendirmesi söz konusu ise işleme faaliyeti hukuka uygun olarak kabul edilmektedir. Üye devletler 13 yaşından daha küçük olmamak şartıyla daha düşük bir yaş belirleyebilmektedir.

Ayrıca tüzükte belirlenen yükümlülüklerin ihlali sonucu olarak öngörülen idari para cezaları da oldukça yüksektir[26]. Nitekim Fransa yakın zamanda tüzüğe dayanarak Google'a dayanarak 57 milyon dolar ceza vermiştir[27].

95/46/EC sayılı Yönerge esas itibariyle, gerçek kişilere ilişkin veriler açısından korunma sağlasa da, üye devletlerin kişisel verilerin korunması mevzuatını tüzel kişileri kapsayacak şekilde düzenlemesine bir engel getirmemiştir. Örneğin İtalya, Avusturya, Danimarka, Lüksemburg tüzel

[24] Dülger, 67.
[25] Develioğlu, 53.
[26] Tüzüğün 83. Maddesinde denetim makamının emirlerine uyulmaması halinde 20.000.000 Euro'ya kadar veya bu miktar yüksekse teşebbüsün bir önceki mali yıldaki toplam yıllık cirosunun %4'üne kadar idari para cezasına hükmedileceği öngörülmüştür.
[27] Uyarer, 56.

kişilere ait verileri korumaktadır. Buna karşılık tüzük sadece gerçek kişilere ait bilgilerin işlenmesi halinde uygulanabilir şekilde düzenlenmiştir[28].

Tüzük ayrıca tüzüğün AB içinde yeknesak ve doğru şekilde uygulanmasını sağlamak amacıyla farklı kurumlar tesis edilmesini ve bunlar arasında iletişim, koordinasyon ve işbirliği yapılmasını öngörmüştür. Avrupa Birliği Koruma Kurulu, hukuki kişiliğe sahip bağımsız bir kuruluş olarak tanımlanmıştır. Ayrıca her bir üye devletin kendi sınırları içinde yetkili bir veya birden fazla bağımsız denetim organı tayin etmesi gerektiği öngörülmüştür. Tüzüğün 70. Maddesinde belirtildiği üzere Kurul, Avrupa Birliği Komisyonuna bu konuda danışmanlık yapmak; kişisel verilerin korunması açısından rehber ve tavsiyeler yayınlamak gibi görevlere sahiptir.

IV- Kişisel Verilerin Ceza Adaleti ve Polis İşbirliği Alanında Kullanılmasına Yönelik Gerçek Kişilere Ait Kişisel Verilerin Yetkili Otoriteler Tarafından Suçların Önlenmesi, Soruşturulması ve Tespit Edilmesi veya Cezaların İnfazı Amacıyla İşlenmesi ve Bu Nevi Kişisel Verilerin Serbest Dolaşımı Hakkında Yönerge

Avrupa Birliği Genel Kişisel Verilerin Korunması Tüzüğüne ek olarak, 2016/680 sayılı Kişisel Verilerin Ceza Adaleti ve Polis İşbirliği Alanında Kullanılmasına Yönelik Gerçek Kişilere Ait Kişisel Verilerin Yetkili Otoriteler Tarafından Suçların Önlenmesi, Soruşturulması ve Tespit Edilmesi veya Cezaların İnfazı Amacıyla İşlenmesi ve Bu Nevi Kişisel Verilerin Serbest Dolaşımı Hakkında Yönerge, 27 Nisan 2016 tarihinde kabul edilmiştir. Yönergenin amacı, 1. maddesine göre yetkili otoriteler tarafından, suçların önlenmesi, soruşturulması ve tespit edilmesi veya cezaların infazı, kamu güvenliğine karşı tehditlerin önlenmesi ve kamu güvenliğinin korunması amacıyla gerçek kişilerin kişisel verileri işlenmesi konusunda onların hak ve özgürlüklerinin korunmasına ilişkin kuralları düzenlemektir.

Yönergenin 2/3 maddesine göre kişisel verilerin Avrupa Birliği Hukukunun uygulanma alanına girmeyen faaliyetler açısından işlenmesi ve Birlik kurumları, organları, birimleri tarafından gerçekleştirilmesi durumunda yönerge hükümleri uygulanmayacaktır. Yönergenin tanımlara ilişkin 3. Maddesinin 7/a-b bentlerine göre yönergeyi uygulaması gereken yetkili makamların suçun önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezai süreçlerin yürütülmesi ile kamu güvenliğinin sağlanması ve kamu güvenliğine karşı tehditlerin önlenmesi hususunda yetkili olan otoriteler olduğu belirtilmiştir. Bununla birlikte, üye devlet hukuku tarafından suçları önleme, soruşturma, tespit etme veya kovuşturma veya kamu güvenliğine yönelik tehditlerin önlenmesi ve bunlara karşı korunma da dahil olmak üzere cezai yaptırımların uygulanması amacıyla kamu otoritesini ve kamu yetkilerini kullanma yetkisi verilen herhangi bir organ veya tüzel kişilik de yetkili makam olarak kabul edilebilmektedir[29].

Yönergede de kişisel verilerin korunması açısından temel prensipler düzenlenmiştir (4md.)[30]. 6. maddede, veri sahipleri arasında farklı kategoriler oluşturmuştur. Veri sahibinin suçla ilgisine ve derecesine bağlı olarak verilerin sınıflandırılması ve ele alınmasının önemini kabul etmektedir. Buna göre kategoriler Şunlardır: ciddi bir suç işleyen ya da işleme şüphesi altında olanlar; bir ceza mahkûmiyetine uğrayan kişiler; bir suç mağduru olanlar ya da suç mağduru olduğuna inanlar; tanıklar. Yönerge böylece, kanunu uygulayan otoritelere farklı kategorideki insanların verileri arasında net bir ayrım yapılmasını öngörmektedir. 8. ve 9. Maddeler ise işlenecek olan verileri ve aynı zamanda işlemin amaçlarını ve bunların bir yasa tarafından belirlenen yetkili makamların görevlerini yerine getirmesi için gerekli olan işlem faaliyetlerini düzenlemektedir[31]. 12. Maddede ilgili kişinin haklarını kullanabilmesi için şeffaf bilgi , iletişim sağlanması ve bunun yöntemleri öngörülmüştür. 13. Maddede veri sahibine bilgi sağlanması ve kişisel verilere erişim hakkı düzenlenmiştir. 14. Maddede kendileriyle ilgili kişisel verilere erişme ve kişisel verilerini içeren mevcut işleme faaliyetleri hakkında bilgi edinme hakkına yer

[28] Develioğlu, 30.

[29] https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L0680&from=it

[30] 4. Maddede veri işleme faaliyetlerinin, amaç sınırlaması, veri azaltması, doğruluk, yasallık, adalet, şeffaflık ile hem dürüstlük hem de gizlilik gereksinimlerini karşılaması gerektiğini belirtmektedir.

[31] Bozbayındır, 76.

verilmiştir.15. maddede erişim hakkının sınırları belirlenmiş tir. 16.madde ise tüzüğün 16. ve 17. Maddelerine benzer şekilde veri sahibine kişisel verilerin düzeltilmesi veya silinmesini isteme ve işlemenin sınırlandırılması hakkını öngörmektedir. 17. Maddede üye devletlerin, veri sahibinin bilgi edinme, kişisel verilere erişme ve düzeltme ya da silinmesini isteme haklarının icrasının yetkili denetim, kontrol otoritesi aracılığıyla sağlayabilecekleri tedbirleri öngörmeleri gerektiği belirtilmiştir.

Tüzükten farklı olarak, yönergede yer alan bütün haklar mutlak değildir ve bunlara cezai soruşturma ve kovuşturmaların gizliliği ve bütünlüğünün korunması ve de sınırsız kullanılmalarının polis ve ceza adalet sistemini işlemez hale getirmesi ihtimaline binaen belli başlı sınırlamalar getirilmiştir. Bunlardan biri, kanuni ve cezai usulleri engellemekten, başkalarının hak ve özgürlüklerini korumaktan veya ulusal ya da kamu güvenliğini sağlamak amacıyla, kontrolörün veri sahibine bilgi sunma yükümlülüğü, bu yükümlülüğün ilgili kişilerin temel hak ve meşru çıkarlarına gereken özeni gösterecek şekilde demokratik bir toplumda gerekli ve orantılı kanunlarla kısıtlanabilmesi, ertelenebilmesi veya ihmal edilebilmesidir. Bu durumda veri sahibi haklarını kullanmaktan mahrum kalabilecektir[32].

Bir diğer önemli fark, işlemenin hukuka uygunluğu açısından veri sahibinin rızasının yönergede yer almamasıdır. Bu açıdan rıza, suçların önlenmesi, soruşturulması, tespit edilmesi veya yargılanması görevlerini yerine getiren yetkili makamlar tarafından kişisel verilerin işlenmesi için gerekli ya da tek başına geçerli bir koşul değildir. Rıza verilerin işlenmesi için hukuka uygunluk nedeni olarak düzenlenmediğinden, ceza adalet makamlarının veri işlemeleri için yasal bir gerekçe oluşturamayacaktır. Verilerin işlenmesi için rıza aranmamakta ise de veri sahibi, üye devletlerin kanunlarına göre, yönergenin amaçları doğrultusunda diğer faaliyetlerde kişisel bilgilerinin işlenmesine onay gösterebilecektir. Örneğin ceza soruşturmalarında DNA testleri ya da cezaların infazında elektronik etiketlerle yerini bildirmeye rıza gösterme mümkündür[33].

Avrupa Veri Koruma Kurulu, tıpkı tüzükle kurulan kurul gibi, üye devletler tarafından yeknesak ve doğru bir şekilde uygulanmasını sağlamak, denetleyici makamlar arasında iş birliğini teşvik etmek, Avrupa Komisyonuna tavsiyelerde bulunmak ve kuralları yayınlamak gibi ile görevleri bulunan; bütün üye devletlerin bağımsız denetim makamları ve Avrupa Veri Koruma denetleyicisinden oluşan bir kuruldur. Ancak tüzükle kurulan Kuruldan farklı olarak, yönergenin 51. maddesinde Kurula kolluk kuvvetleri alanında merkezi bir rol biçilmemektedir. Yönerge, her üye devletten bir ya da birden fazla kamu yetkilisinin yönergenin uygulanmasını izlemek için görevlendirilmesini talep etmektedir. Bu gözetim, kişilerin temel hak ve özgürlüklerinin sağlanması ve Birlik içinde verilerin güvenli bir biçimde serbest akışının sağlanmasını amaçlamaktadır.

Yönergenin 52. Maddesinde veri sahibinin, verilerinin işlenmesi sırasında yönerge kurallarına aykırılık nedeniyle bağımsız denetim makamına şikayet etme hakkı düzenlenmiştir. 53 ve 54. Maddelerde ise hem denetleyici otoriteye hem de veri sorumlusu ve işleyenlerine karşı etkili bir yargı yoluna başvurma hakkı da öngörülmüştür. 57 ve devamı maddeler inde ise üye devletlerin veri sahibinin maddi ve manevi zararlarından dolayı tazminat talep etme haklarını tanımaları ve ihlali gerçekleştiren tüzel ya da gerçek kişilere karşı etkili, orantılı ve caydırıcı cezalar uygulamaları gerektiği düzenlenmiştir[34].

Sonuç olarak, yönergenin AB içinde kişisel verilerin ceza adalet mekanizmalarında korunması açısından standartları belirlemede önemli bir adım olduğunu; bu konuda bireylerin

[32] Bozbayındır, 78.

[33] Bozbayındır, 80.

[34] Bozbayındır, 88.

hakları ile adli ve polis adalet sürecinin gereklilikleri arasında bir denge tutturmaya çalıştığını söylemek mümkündür[35].

[35] Benzer görüş için bkz. Bozbayındır, 97.

FIGHT AGAINST CYBER CRIME IN REPUBLIC OF SERBIA*

Branko Lestanin, PhD candidate, Faculty of Nis
Ministry of Interior, Serbia
b.lestanin@gmail.com

Prof. Zeljko Nikac, PhD
University of Criminal Investigation and Police Studies, Belgrade, Serbia
zeljko.nikac@kpa.edu.rs

***Abstract*:** Computers and computer systems are an integral part of people's lives in modern society, without which many of their activities are unimaginable. This particularly applies to the Internet and other social networks that use millions of people all over the world in everyday life and work, and among them are especially young and even children. In addition to numerous advantages of using computers, it has its own negative side, which is reflected in the alienation of personality, violates privacy, and especially in the commission of felonies by the abuse of computers, computer systems and social networks.

The paper points the fight against cybercrime in the Republic of Serbia as a country that is now in transition. In short, the international legal framework and more important international documents in this area, as well as the national legal framework for combating criminal activities in the field of cyber (computer) crime, are exposed. More detailed are the most important crimes from the Criminal Code of the Republic of Serbia, which have criminalized certain unlawful behavior and provided sanctions for perpetrators of felonies. In the function of the topic, it was also pointed out to the more important general and special evidence procedures from the Criminal Procedures Code that are of importance for the processing of cybercrimes and perpetrators.

The operational aspect of the fight against cyber crime starts from the most important subjects in the Republic of Serbia - a special Police Department within the Serbian Organized Crime Police Service and a special Department of Public Prosecution within the Republic Public Prosecutor's Office. Specialized bodies have relatively good human and material resources to combat this extremely dangerous form of crime, where criminalistics' IT and forensics have a special place in the process of obtaining relevant evidence for the processing of perpetrators.

In conclusion, some *de lege ferenda* proposals are given with the aim of improving the legal and institutional framework for the suppression of cyber crime.

***Key words*:** cyber crime, international legal framework, criminal legislation, Serbia and the EU

INTRODUCTION

Computers and computer systems are an integral part of people's lives in modern society, without which many activities are simply unthinkable. This is especially true for the Internet and other social networks used by millions of people around the world in their daily lives and work, with young people and even children in particular. Modern society is simply unthinkable without information technologies that have entered into all spheres of social life, and this is supported by

* This paper is the result of the research on Project *Development of institutional capacity, standards and procedures for countering organized crime and terrorism in the conditions of international integration,* Ministry of Education and Science of the RS No. 179045.

their enormous development and application in all business activities and private life of people. This is especially true for smart phones, tablets, smart TVs and other devices that include microprocessors and software that allow them to practically become computers. People have started to refer to this era as the 'converged environment', i.e. a situation where we seamlessly swap between the online and offline worlds without really noticing.[1] In addition to its numerous advantages, the use of computers has its negative side, which is reflected in the alienation of the person, the violation of privacy and especially the commission of criminal offenses through the misuse of computers, computer systems and social networks.

The form of cybercrime that we encounter today binds to the development of telecommunications media and modems during the 1960s, when the first technically educated delinquents began to develop methods and means for the unauthorized use of telephone services. At that time, the first computer programs were designed to invade other people's systems ('worms', 'viruses', 'trojan horse').[2]

The social response to cybercrime is taking place nationally and internationally and includes measures at the legislative and operational levels. Internationally, states and international organizations have adopted significant international instruments (conventions, resolutions, declarations) that treat cybercrime as an international problem, requiring international reaction and cooperation from states. States have committed themselves to harmonizing domestic law with international norms and participating in international cooperation in the fight against cybercrime. The operational response encompasses activities, measures and actions at national and international levels to combat cybercrime. This applies above all to information sharing, joint operations and other actions, joint investigative teams and all forms of cooperation in comating cybercrime.[3]

The Republic of Serbia, like other countries in transition, has faced the rapid development of information technologies and therefore cybercrime, as an inevitable consequence of this process. In general, the national normative framework can be judged to be in line with international law because the Criminal Code (CC)[4] criminalizes computer crime. In addition, other, primarily organizational, legal and regulatory provisions, regulate the area of combating cybercrime. National regulations set up specialized bodies for combating high-tech crime, which are made up of special departments of courts, prosecutors' offices and police, employing law enforcement personnel trained in this field.[5]

INTERNATIONAL LEGAL FRAMEWORK FOR THE FIGHT AGAINST CYBER CRIME, THE REVIEW

In a broader sense, the international legal framework to combat cyber crime includes legal acts ratified at the universal level (UN and their specialized agencies) that are widely used. In a narrow sense, this framework implies certain legal acts of a regional character at European level (EU, SE). The analysis of the norms of these legal acts can determine that they cover the issues of combating the most serious forms of crime, international criminal-legal cooperation and international police cooperation.

---

[1] Alisdair Gillespie, *Cybercrime: Key Issues and Debates* (2nd edn, Routlidge 2019) 6

[2] Jozo Čizmić, Marija Boban, 'Electronic Evidence in the Judicial Proceedings and Computer Forensic Analysis' 38 (2018) PFLUS 23, 30

[3] Ž Nikač, *Međunarodna policijska saradnja* (Kriminalističko-policijska akademija 2015) 109-112 [Eng. *International Police Cooperation*]

[4] Criminal Code, Official Gazette of RS, No 85/05, 88/05-cor., 107/05-cor., 72/09, 111/09, 121/12, 104/13, 108/14, 94/16 and 35/19

[5] Law on Organization and Jurisdiction of State Bodies for Combating High-Tech Crime, Official Gazette of RS No 61/05 and 104/09 (High-Tech Law)

Broadly speaking, significant international documents in the fight against cybercrime are: United Nations Convention against Transnational Organized Crime,[6] Police Cooperation Convention for Southeast Europe[7] and Convention of the Southeast European Law Enforcement Center.[8] At the 8th UN Congress on Crime Prevention and Treatment of Offenders (1990), a Resolution on Computer Crime was adopted, which is considered to be a significant UN act in this area. In 2000, the UN General Assembly adopted a Resolution on combating the misuse of information technology, which was revised in 2001.[9] In a narrow sense we can point out the legal acts of the Council of Europe and the European Union as Convention on Cyber crime of the Council of Europe (CETS No.185)[10] from 2001 adopted in Budapest, signed and ratified by the Republic of Serbia by a separate Law on Ratifying the Convention on High-Tech Crime[11]. For the implementation of the Convention in 2003 in Strasbourg the Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems was adopted.[12]

The EU, as a community of independent states, has adopted several important documents in the area of combating cybercrime. Chronologically, the first adopted was the Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC[13] for more effectively combat cybercrime based on electronic clues and other evidence. Then the Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs[14] was adopted, which is focused on copyright and intellectual rights in the virtual world. In addition, several secondary legislation has been adopted to implement these directives. We will bring up just last one the Directive 2013/40/EU of the European parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.[15]

In the procedural sense, it is also important to mention the European Arrest Warrant (EAW), which was adopted by Council of the EU (2002), Framework Decision of 13 June 2002 on the European arrest w[16]arrant and the surrender procedures between member states, 2002/584/JHA.[17] The EAW is a substitute for extradition, which annuls the political aspect of extradition

---

[6] United Nations Convention against Transnational Organized Crime (UNCATOC) <https://www.unodc.org/unodc/treaties/CTOC/ > accessed 20 July 2019

[7] Police Cooperation Convention for Southeast Europe (PCCSE), <http://www.pccseesecretariat.si/index.php?item=9&page=static, PCC SEE 2006 2011.pdf > accessed 20 July 2019

[8] SELEC Convention, <http://www.selec.org/docs/PDF/SELEC%20Convention%20%5Bsigned%20on%2009.12.2009%5D.pdf > accessed 20 July 2019

[9] Zdravko Grujic, 'Cybercrime: Specificity and Contemporary Challenges' 57 (2018) CPFLN 325, 333

[10] Convention on Cybercrime, CETS 185, 23 November 2001 <http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_.pdf > accessed 20 July 2019; Furder readings in Gillespie (n 1) 19-22

[11] Law on Ratifying the Convention on High-Tech Crime, Official gazette RS No 19/09

[12] < https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f > accessed 20 July 2019; Further readings in Gillespie (n 1) 23-22; Miomira Kostic, Vida Vilic,'Measures for Protection the Right to Privacy According to Council of Europe Convention on Cybercrime', (2012) 58 CPFLN 83

[13] Directive 2006/24/EC, Official Journal of the European Union, L 105/54, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0024 > accessed 20 July 2019

[14] Directive 2009/24/EC, Official Journal of the European Union, L 111/16, < http://eur lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009L0024 > accessed 20 July 2019

[15] Directive 2013/40/EU of the European parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:en:PDF > accessed 20 July 2019

[16]

[17] Council of the EU (2002), Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between member states, 2002/584/JHA, Official Journal L 190, 18/07/2002;< http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002F0584:EN:HTML > accessed 20 July 2019

proceedings and leaves cooperation in criminal matters to the competent courts. In order to implement this instrument of judicial cooperation, the principle of mutual recognition of judicial decisions has come to the fore. Member States have undertaken to respect the decisions of foreign judicial instances, to accept and enforce them in their territory without formalism.[18]

In the harmonization of the national legal framework, it is especially important to analyze the provisions of international legal acts, then the definitions of certain terms used in the field of cybercrime, legal institutes to be harmonized, criminal and other sanctions.

NATIONAL LEGAL FRAMEWORK FOR COMBATING CYBER CRIME IN SERBIA

In addition to the aforementioned laws, from the aspect of the fight against cybercrime in the legislative framework of Serbia, other regulations in the criminal law and police-legal fields, which have substantive, procedural and organizational legal character, also occupy an important place. These include first and foremost Criminal Procedure Code[19] (CPC), Police Law[20], Law on organization and jurisdiction of state bodies in combating organized crime, terrorism and corruption,[21] and Law on Forfeiture of Property Arising from Criminal Offense[22].

The aforementioned Convention obliged States Parties, and therefore Serbia, to provide for the following offenses in national legislation: 1) Offences against the confidentiality, integrity and availability of computer data and systems; 2) Computer-related offences; 3) Content-related offences; and 4) Offences related to infringements of copyright and related rights.[23]

a) Material criminal legislation

According to the available historical and legal data, cybercrime crimes were introduced into the criminal legislation of Serbia by the 2003 novelties,[24] with a later codification of the material criminal legislation of 2005[25] to become an integral part of it. Today, cybercrime offenses are listed in Chapter XXVII of the CC under the title 'Crimes against the security of computer data', namely: 1) Damage to computer data and programs; 2) Computer sabotage; 3) Creating and introducing computer viruses; 4) Computer fraud; 5) Unauthorized access to a protected computer, computer network and electronic data processing; 6) Impeding and limitation access to a public computer network; 7) Unauthorized use of computers or computer networks; and 8) Creating, procuring and providing other means for committing criminal offenses against computer data security.[26]

The criminal sanctions for these offenses range from a fine or imprisonment of till three months[27] (Article 304, paragraph 1 of the CC) as the tender sentence, to imprisonment of up to ten years (Article 301, paragraph 3 of the CC) as the most severe sentence. The imposition of a security measure forfeiture of items is mandatory and applies to devices and means of the criminal offense (personal computer, laptop, etc.), with the condition that the items are the property of the perpetrator for certain criminal offenses. Except for the criminal offense 'Unauthorized use of a

[18] Božić, Knežević, Nikać, 'European Arrest Warrant as a Mechanism of Extradition in International Criminal Justice Cooperation' 57 (2018) CPFLN 15, 18
[19] Criminal Procedure Code, Official gazette of RS, No72/11, 101/11, 121/12, 32/13, 45/13, 55/14 and 35/19
[20] Police Law, Official Gazette of RS, No 6/16, 24/18 and 87/18
[21] Law on organization and jurisdiction of state bodies in combating organized crime, terrorism and corruption, Official Gazette of RS, No 94/16.
[22] Law on Forfeiture of Property Arising from Criminal Offense, Official Gazette of RS, No 32/13 and 94/16.
[23] Articles from 2 to 10 Convention on Cyber crime
[24] Law on Amendments and Supplements of Criminal Code, Official Gazette No 67/03
[25] Criminal Code, Official Gazette No 85/05
[26] Articles from 298 to 304a CC
[27] Here is applied the general statutory minimum prison sentence in Serbia than thirty days (art. 45 para. 1 of the CC)

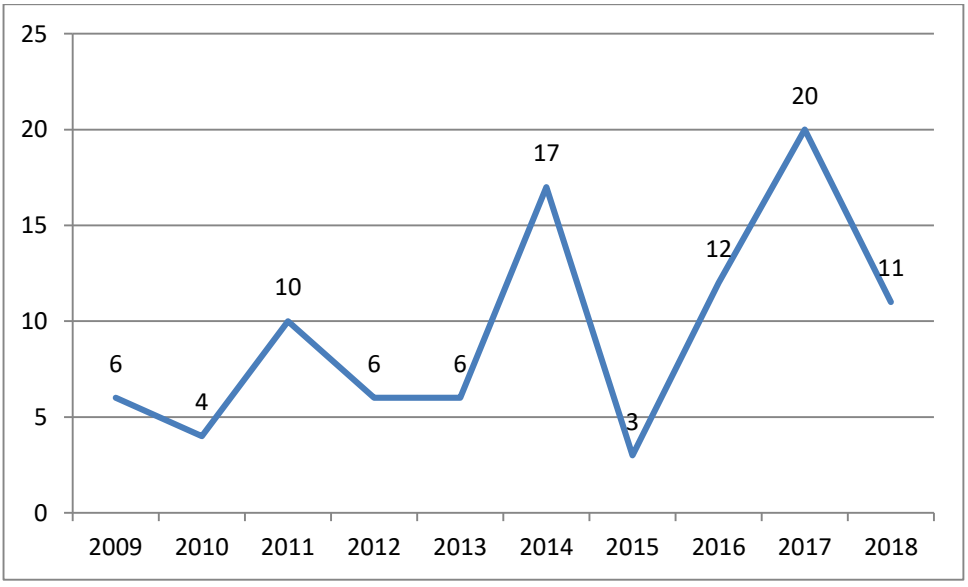
computers or computer network' (Article 304 CC) for which prosecution is initiated in a private lawsuit for all other criminal offenses shall be prosecuted ex officio.

Criminal offenses of high-tech crime, excluding incriminations from the group against the security of computer data, within the meaning of the High-Tech Law, shall include: 1) criminal offenses against (intellectual) property, economy and legal system, where computers, computer networks occur, computer data as well as their products in physical or electronic form – if the number of copyright copies exceeds 2,000 or if the material damage exceeds the amount of RSD 1,000,000; 2) criminal offenses against the freedoms and rights of man and citizen, sexual freedom, public order and peace and the constitutional order of the Republic of Serbia, which, by reason of the modus operandi or the means used, can be concluded to be acts of high-tech crime, for sure.[28]

Bearing in mind the national legislative framework, cybercrime in Serbia can be conditionally viewed in a narrower and broader sense. In the narrower (criminal law) sense cybercrime covers only criminal offenses against the security of computer data, while in the broader (functional) sense cybercrime covers all criminal offenses where information technologies occur with the object or means of execution and with high material damage, or if the modus operandi indicates the cybercrime. In other words the broader sense is actually the High-Tech crime.

Empirical studies of cybercrime in Serbia show that this type of crime does not occupy a significant place in the total detected and prosecuted crime. According to the Statistical Office of the Republic of Serbia in the period 2009-2018 a total of 95 persons have been reported for computer security criminal offenses (cybercrime in the narrowed sense). Out of the total number of perpetrators reported, 49 were found guilty and sentenced which is 51.58%, while 12 perpetrators were sentenced to imprisonment as the most severe sentence, which is about 24.49%.[29] Looking individually by year (Chart 1), we can see different trends and development of cybercrime over a ten-year period. The highest number was in 2017 (20) while the smallest number was in 2015 (3), which is almost seven times less and the average number of perpetrators is 10 per year.

Chart 1 – Reported cybercrime perpetrators from 2009 till 2018



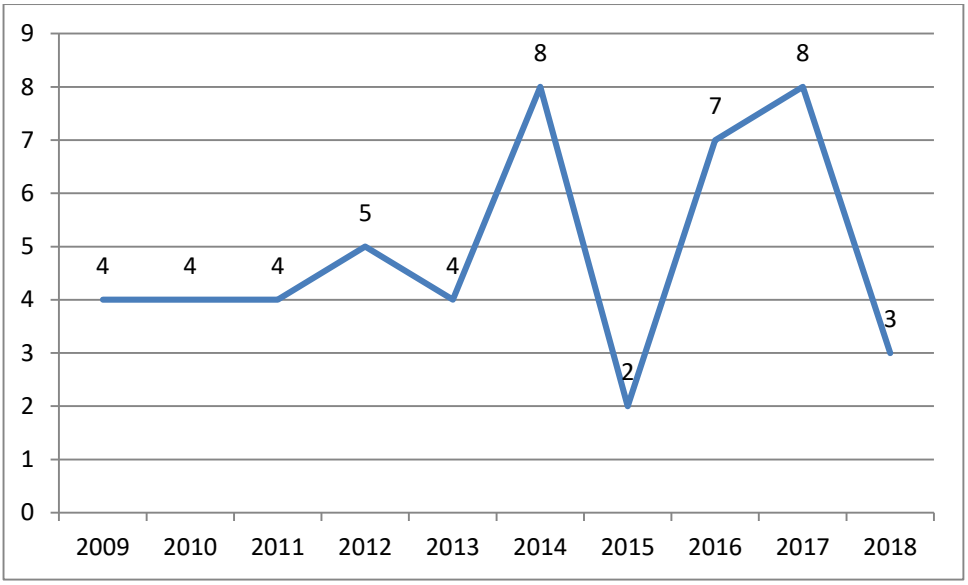
Source: Statistical Office of the Republic of Serbia

The analysis of convicted persons for cybercrimes (Chart 2) shows slightly different tendencies in the work of judicial authorities, but based on the presented data it can be concluded that the

[28] Ivana Bodrozic, 'Criminal Offences with Elements of High-Tech Crime' 55 (2013) Bezbednost 142, 144
[29]< http://www.stat.gov.rs/oblasti/pravosudje/punoletni-ucinioci-krivicnih-dela/ > accessed 23 July 2019

increase in the number of reported perpetrators is accompanied by an increase in the number of convicted perpetrators. The maximum number of convicted perpetrators was observed in 2014 and 2017 (8), while the lowest number of convicted perpetrators was 2015 (2). Comparing to the previous chart, we see that in 2017 there were the highest number and 2015 the lowest number of reported perpetrators.

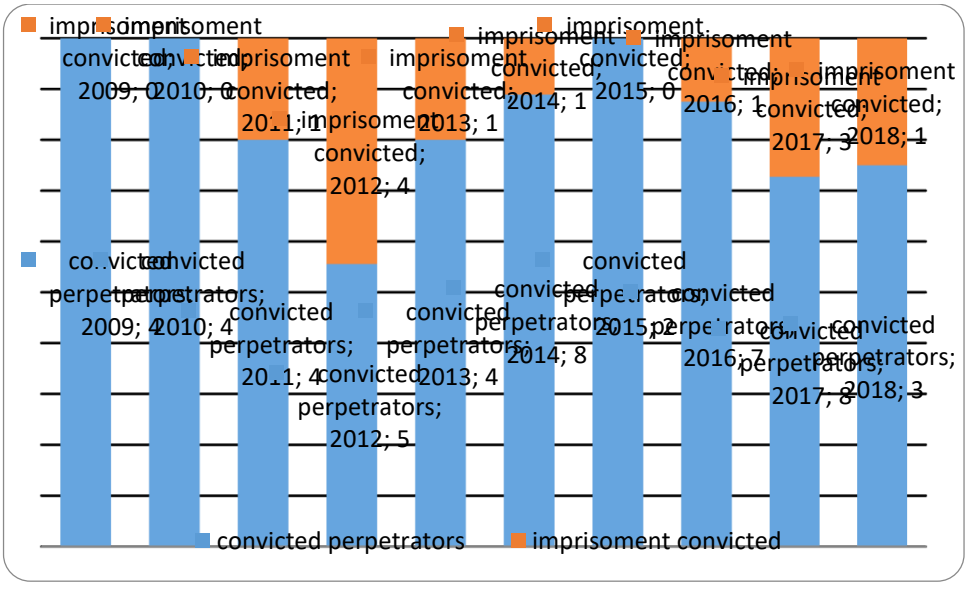
Chart 2 – Convicted cybercrime perpetrators from 2009 till 2018



Source: Statistical Office of the Republic of Serbia

The current (material) criminal legislation issues for certain forms of cybercrime the imprisonment as the most severe sentence, but only a quarter of the total number of convicted perpetrators have been sentenced to prison. Analyzing by years, we see that the courts in Serbia were the most stringent in cybercrime cases in 2012 and the mildest in 2019, followed by 2010 and 2015 when no prison sentence was imposed (Chart 3). On average, courts in Serbia each sentence one year in prison for cybercrime.

Chart 3 – Imprisonment imposed in the period 2009-2018



Source: Statistical Office of the Republic of Serbia

b) Proceedings legislation

The criminal procedure in Serbia is divided into several stages in which the authorized state bodies play their role. The first stage is the pre-trial procedure, which is managed by the public prosecutor, and which, together with the police, works on the detecting and clarifying of criminal offenses through the use of operative-pursuit (exceptionally and evidentiary) measures. The second phase is an investigation in which the public prosecutor, with the help of evidentiary measures (general and special), builds the factual basis of a future indictment. The third stage is the main criminal procedure, which is within the jurisdiction of the court, which seeks to resolve the criminal matter and reach a judgment. The fourth stage, which is of a facultative nature, is the procedure for regular and extraordinary legal remedies. Criminal proceedings can be conducted as a regular one if it is a criminal offense for which a sentence of imprisonment of more than 8 years is issued and as shorten (summary) proceedings for criminal offenses for which a fine or imprisonment of less than 8 years can be imposed.[30]

Cybercrime is a special type of criminal act that requires specific operational-pursuit and evidentiary measures. Operational-pursuit measures are issued in Art. 286-294 of the CPC, and from the aspect of cyber crime, we will mention only the most important. The police must first collect the necessary information from all persons who have any knowledge of a specific cybercrimes. In particular, the collection of information should be directed to the victims, who, when undertaking this measure, must collect information on the time, place and modus operandi, data on the devices used, the origin and mode of use of the devices, access to the Internet, the use of virtual data warehouses (clouds), using encryption and so one.[31]

Additionally with the request of the public prosecutor and with the order of the preliminary procedure (pre-trial) judge, police can obtain records of recorded telephone communications, the base stations used or make the locating spot from which the communications is conducting. This measure consists in determining the so-called the formal characteristics of communication without going into the specific content of communication. The listing can determine the source and destination of the communication, the type of communication (call, message, data exchange), the beginning, duration and termination of communication, the place from which the communication was made, the base station from which the communication was made and the mobile phone identification (IMEI) number. Given that it can be applied only on the order of a pre-trial judge, this 'operative' measure should be issued as a (general) evidentiary measure and that the information gathered by this measure can be used as evidence in the court proceedings.[32] Bearing in mind that the Public Prosecutor is the head of the pre-trial phase of criminal proceedings, the police are obliged to immediately inform him/her of the actions taken, and within 24 hours at the latest. Considering prosecutorial-police practice, this notification is realized by telephone by informing the on-duty public prosecutor.

Evidentiary measures, by the rule, are executed at the investigation stage but can also be executed at the pre-investigation stage. They are generally divided into general and specific evidentiary measures. For the purpose of proving cybercrimes, the first step is an evidentiary measure of insight (Article 133-136 CPC), an insight of items (Article 135) that is undertaken when it is necessary to establish or clarify a fact in the proceedings with directly observation of police or

[30] By abstraction from the CPC provisions, it can be concluded that the specifics of the summary proceedings are reflected in the specific grounds for detention, the type of the indictment, the judicial control of the prosecution, the special prerequisites for holding the main trial where the defendant's confession is crucial, the judgment is immediately pronounced and published and the specific procedure for remedies.

[31] As evidence in legal proceedings may be used, and printed text generated by the computer itself, or it is only archived (so-called handwriting of a person in electronic form), text processed by e-mail processors, records from activities of discussion groups (forums and blogs) and virtual chat rooms, provider logs related to user identification (internet protocols), telephone records, voice recorders, etc. According to Čizmić, Boban n2, 38

[32] Muamer Nicevic, Branko Lestanin, 'Proposals of Amendment of the Serbian CPC in Order to Improve Policing' 56 (2018) JCCL 127, 135

public prosecutor over movable and immovable property of defendant or other persons. In cybercrime cases, these are usually things used to commit a crime or that carry information or traces of a crime (computer, lap top, mobile phone, tablet, Wi-Fi routers, etc.).

With regard to the evidentiary measures, it is necessary to consider the issue of computer insight, since the legislature is introducing a special search operation for automatic data-processing devices, as well as equipment on which electronic records are stored (which it is intended to be undertaken on the basis of court warrant and, if necessary, with the assistance of an expert, pursuant to Article 152 para. 3 of the CPC) opened a new chapter in dealing with such devices in the procedural sense. The problem that can be intensified here is related to the understanding of the device, which in this work can generally be defined as a computer, because it can also be understood as a communication tool from which, at the time of processing (in terms of providing a place, insight and search), communication, which may include the competences of other entities and those of other States. Generally, this measure could be determined, according to the most widespread form of understanding (encroachment on rights and freedoms), collectively called the search of computers and devices of carriers of digital traces. In our constellation of measures in the CPC, this is neither a pursuit measure nor a special evidentiary measure, but an evidentiary measure.[33]

Considering that cybercrime perpetrators as a primary objective in most cases have the acquisition of unlawful material gain, the evidentiary measure of 'Checking accounts and suspicious transactions' is particularly significant. It consists in the acquisition of information, the supervision of suspicious transactions and the temporary suspension of a suspicious transaction ordered by a public prosecutor and directly executed by a bank or other financial organization. As a condition for taking this evidentiary measure, it is necessary for the suspect to have accounts or carry out transactions and that there are grounds for suspicion that (s)he has committed a criminal offense punishable by four years imprisonment or a severe sentence or other offenses of a corrupt and pornographic character. Therefore, in cybercrime sense, this measure can only be taken for the following: 1) the qualified form of Computer Data and Program Damage Art. 298 para. 3 CC; 2) Computer sabotage Art. 299 CC; and 3) qualified forms of Computer fraud Art. 301 para. 2 and 3 CC.

Other general evidentiary measures that are particularly relevant to detecting, clarifying and proving cybercrime are: the search of persons, apartments and other premises; temporary seizure of items; questioning the witness and the suspect and questioning the defendant. When taking these measures, the most important thing is to preserve the credibility of the electronic evidence. Work on the direct fixation and collection of electronic evidence is carried out by expert and trained police officers. What would be of particular help in collecting electronic evidence is finding notes or scrips containing passwords or instructions for using certain types of software. In particular, we must be careful when handling the computer or laptop. Disconnected devices and those that are already turned off should not be turned on; the laptop with the lid closed can be opened and checked to see if it is active. Secure storage devices (flash drives, hard drives, etc.) have to fixed with a photo and describe it in a temporary seizure certificate and do not attempt to view content through a computer or laptop, unless professionally employed.

Special evidentiary measures constitute an exception and are executed for specific criminal offenses and if formal and material conditions are met. The *formal requirement* is the existence of a reasoned warrant of the pre-trial judge, which is issued on the proposal of the public prosecutor.[34] *Material condition* refers to the criminal offense and obstacles to proving it. Specific

[33] Zvonimir Ivanović, 'Issue of dealing with digital evidence in Serbian legislative' 2 (2015) CTP 7, 11

[34] The role of the police is in initiating the procedure of issuing a pre-trial judge's order to take a special evidentiary measure has not been formally determined and is reflected in the presentation of intelligence, grounds for suspicion and the filing of an initiative to the public prosecutor. In terms of their realization, the police execute all special

evidentiary measures may be ordered when two conditions are met, one relating to the type of criminal offense[35] and the other to the existence of appropriate evidentiary difficulties. This means that at the same time, the following two conditions must exist: 1) the existence of grounds for suspicion that criminal offense has been committed that falls into the category of criminal offenses in respect of which special evidentiary measures are possible ('special criminal offense'); 2) it is necessary that no evidence of criminal prosecution can be collected in another way or would be significantly impeded. Special evidentiary measures may also be exceptionally assigned to a person for whom we have grounds to suspect that preparing one of the 'special criminal offenses' if there are two alternatively issued conditions: 1) when the circumstances of the case indicate that the criminal offense could not otherwise be detected, prevented or proved; 2) when detection, prevention or proving process would cause disproportionate difficulty or great danger.[36]

In detecting, clarifying and proving cybercrime, using the computerized (raster) search (Articles 178-180 CPC) is particularly specific. It involves the computer search of already processed personal and other data and their comparison with the data relating to the suspect and the crime. In particular, the data stored in the databases of other state bodies to which the police do not have direct access (tax administration, local self-government, ownership and other forms of real rights over real estate, movable property, etc.) are searched here. In other words, access to computer systems and computer reconciliation refers to the comparison of citizens' personal data processed in appropriate databases, with data and registers contained within police records.[37] From the point of view of cybercrime, the databases of providers of internet services, internet sales, central database of social networks, etc. are particularly interesting. When initiating the implementation of this measure, one must be especially careful and specify to the public prosecutor exactly what data is being searched and for what purpose. In one of its decisions, the European Court of Human Rights concluded that the search and review of all electronic data constituted 'more than was necessary to achieve a legitimate aim', which led to the conclusion that there was a violation of Article 8 of the European Convention in this case.[38]

In order for the computer data to be used as evidence in criminal proceedings, it must be established that they were collected and processed in accordance with the law (*legality requirement*), that there was no intentional or accidental alteration/loss of electronic records, or that the records were presented as evidence before court no more or less in relation to the time when they were collected (*condition of authenticity*) and that they are eligible to determine the existence and truth of a particular fact in criminal proceedings (*condition of relevance*).[39]

Police powers referring to proceedings after a criminal offense or misdemeanour (investigative powers) are primarily issued by criminal or misdemeanour legislation, while those having preventive character or strictly 'police powers' are part of police legislation.[40] In terms of cybercrime, the preventative role of the police is very significant, which through various

---

evidentiary measures with the fact that the security services, customs, tax authorities, etc., are authorized to apply them.

[35] These include cybercrime (*auth. rem.)*

[36] Milan Škulić, 'Tajni audio i video nadzor kao posebna dokazna radnja u Zakoniku o krivičnom postupku Srbije' 28 (2015) TR 24, 39 [Eng. Secret Audio and Video Surveillance as Special Evidentiary Action in Criminal Proceedings Code of Serbia]

[37] Saša Knežević, *Krivično procesno pravo: opšti deo* (Pravni fakultet Niš, 2017) 337 [Eng. *Criminal Proceedings Law: general part*]

[38] Goran Ilić, Marina Matić Bošković, *Posebne mere tajnog prikupljanja podataka u krivičnom postupku : pogled iz pravosuđa*, (Beogradski centar za bezbednosnu politiku, 2015) 14 [Eng. *Special Measures of Secret Data Collection in Criminal Proceedings: The View from Judiciary*]

[39] Paraphrased according to Milana Pisarić, 'Search of Computers for Discovery of Electronic Evidence' (2015) 49 CPFLNS 215, 217

[40] Branko Leštanin, Željko Nikač, *Komentar Zakona o policiji* (Poslovni biro, 2016) 144 [Eng. *Commentary of Police Law*]

counselling, forums and contacts with citizens can influence the raising of awareness on internet security.[41] An example is the so-called 'Click Safely' campaign, which focuses primarily on the safety of children increasingly using the Internet.[42] However, if the crime did occur, the first answer is especially important where the police have a primary role to play in securing the crime scene. The security of the crime scene is applied by the first police officer who is dispatched to the crime scene, or who finds him/herself there, to secure it and who manages the security of the crime scene until the arrival of the insight team (public prosecutor, criminal police, forensics, etc.).[43] Particular attention should be paid to IT devices to computer, laptop, tablet, mobile phone, Wi-Fi router, etc. The most important thing is that during the securing of crime scene, nothing should be touched, prevent of all persons to come into contact with IT devices, notice the situation on the spot, the position of the laptop, the cable for the Internet, etc.

FIGHTING CYBER CRIME IN BOSNIA AND HERZEGOVINA AND MONTENEGRO, COMPARATIVE LEGAL REVIEW

In this part of the paper, we will briefly look at the material criminal legislation of some Western Balkan countries, more specifically the countries that were members of the former Yugoslav Federation.

a) In the context of comparative legal analysis, we first point out that Bosnia and Herzegovina has a specific state and legislative organization, because there are three levels of state and legal system: central, entity and local (cantonal). The Criminal Law of Bosnia and Herzegovina[44] (CLBIH) does not provide specific criminal offenses in the area of cybercrime, but considers the computer system as a separate material element of three criminal offenses: Unauthorized wiretapping and audio or optical recording (Article 147a para. 1), Illicit weapons trafficking and military equipment and dual-use products (Article 193 para. 2) and Illicit Use of Copyright (Article 243 para. 3) of the CLBIH.

Considering the provisions of the Criminal Law of the Federation of Bosnia and Herzegovina[45] (CLFBIH), criminal offenses related to information technologies are listed in Chapter XXXII 'Crimes against the Electronic Data Processing System', namely: 1) Damage to computer data and programs; 2) Computer forgery; 3) Computer fraud; 4) Obstruction of the system and network of electronic data processing; 5) Unauthorized access to a secure system and electronic data processing network; and 6) Computer sabotage.[46] When it comes to criminal sanctions for the listed offenses, they range from a fine or imprisonment till one year[47] (Article 393 para. 1 of the CLFBIH) to a maximum of twelve years (Article 395 para. 3 of the CLFBIH) and seizure of a items without any additional conditions. All offenses are prosecuted ex officio.

The provisions of the Criminal Law of Republic of Srpska[48] (CLRS) in Chapter XXXII, titled 'Crimes against the Security of Computer Data', lists the following criminal offenses: 1) Damage to computer data and programs; 2) Computer sabotage; 3) Creation and introduction of computer viruses; 4) Computer fraud; 5) Unauthorized access to a secure computer, computer network, telecommunication network and electronic data processing; 6) Preventing and restricting access

[41] Further readings in Željko Nikač, *Policija u zajednici* (Kriminalističko-policijski univerzitet, 2019) [Eng. *Community policing*]; Miroslav Bača, Jasnim Ćosić, 'Preventing Cyber Crime', 22 (2013) PS 146
[42] <https://kliknibezbedno.wordpress.com/ > accessed 22 July 2019
[43] Leštanin, Nikač n39, 216
[44] Criminal Law of Bosnia and Herzegovina, Official Gazette of BIH, No 3/03, 32/03 - cor., 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 8/10, 47/14, 22/15, 40/15 and 35/18
[45] Criminal Law of Federation of Bosnia and Herzegovina, Official Gazette of FBIH, No 36/03, 21/04 - cor., 69/04, 18/05, 42/10, 42/11, 59/14, 76/14, 46/16 and 75/17
[46] Articles 393 – 398 CLFBIH
[47] Here the general statutory minimum prison sentence in the entity of thirty days is applied (art. 43 para. 1. CLFBIH)
[48] Criminal Law of Republic Srpska, Official Gazette of RS, No 64/17 and 104/18 – desi. CC

to the public computer network; and 7) Unauthorized use of a computer or computer network.[49] Republic of Srpska criminal legislation more closely looks at cybercrime, so when it comes to criminal sanctions for the listed offenses, they range from a fine or imprisonment till six months[50] (Art. 409 para. 1, 410 para. 4, 411 para. 1 and 413 para. 1 of the CLRS) up to a maximum of ten years (Article 410, para. 3 of the CLRS), with mandatory seizure of items from criminal offense without additional conditions. For all criminal offenses the prosecution shall be undertaken ex officio, with the exception of criminal offense 'Unauthorized Use of a Computer or Computer Network' Art. 413, for which the prosecution will be undertaken on the proposal of the victim.

b) The criminal legislation of Montenegro is also interesting for legal analysis from the aspect of cybercrime. The Criminal Code of Montenegro[51] (CCM) in Chapter XXVIII, titled 'Crimes against the Security of Computer Data', issues the following criminal offenses: 1) Damage to computer data and programs; 2) Interference with the computer system; 3) Creating and introducing computer viruses; 4) Computer fraud; 5) Unauthorized access to the computer system; and 6) Misuse of devices and programs.[52] The criminal sanctions issued for the aforementioned offenses range from a fine or imprisonment to one year[53] (Art. 349 para. 1, 351 para. 1, 353 para. 1 and 354 para. 2 of the CCM) as a minimum sentence of up to 12 years imprisonment (Art. 352 para. 3 of the CCM) as the maximum issued sentence. The objects used for the commission of the crime must be confiscated, provided that for certain criminal offenses the condition is that the objects are the property of the perpetrator. All cybercrime offenses are prosecuted ex officio.

OPERATIONAL ASPECTS OF THE FIGHT AGAINST CYBER CRIME IN SERBIA

In the Republic of Serbia, the most important authorities in the fight against cybercrime are the Special Department for Combating High-Tech Crime (HT Police) within the Office for Combating Organized Crime in Serbian Criminal Police, and then the Special Department for Combating High-Tech Crime within the Higher Public Prosecutor's Office in Belgrade (Special Prosecutor's Office), and especially the High-Tech Crime Division within the Belgrade Higher Court.

The jurisdiction of the Special Prosecutor's Office is related to the Prosecutor's Office of the Republic of Serbia since the special prosecutor appointed by the Republican Public Prosecutor and of the order of Deputy Republican Public Prosecutors who are eligible for election as deputy higher public prosecutor. Priority in selection is given to deputy public prosecutors who have specific knowledge in the field of information technology. An empirical study (Chart 4) in Serbia shows an increase in the activity of the Special Prosecutor's Office in the prosecution of cybercrime (in a broad sense). In the period 2013-2017, a total of 1,318 criminal charges were filed with the Special Prosecutor's Office against adults, of which 280 persons were prosecuted (21%).[54]

Chart 4 – Number of cases in Special Prosecutor's Office

[49] Articles 407 – 413 CLRS

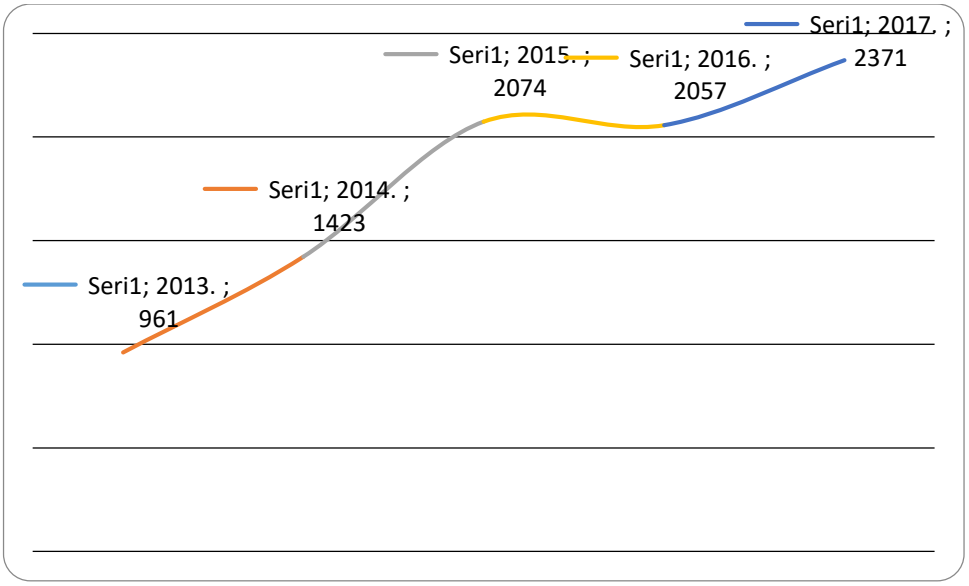
[50] The general statutory minimum sentence of imprisonment in an entity of three months applies here (Art. 46 para. 1 CLRS)

[51] Criminal code of Montenegro, Official Gazette of RM, No 70/03, 13/04 - cor. and 47/06 and Official Gazette of MNE, No 40/08, 25/10, 32/11, 64/11 – other law, 40/13, 56/13 - cor., 14/15, 42/15, 58/15 – other law, 44/17 and 49/18

[52] Articles 349 – 354 CCM

[53] The general legal minimum of thirty days' imprisonment in Montenegro applies here (Article 36 para. 1 of the CCM)

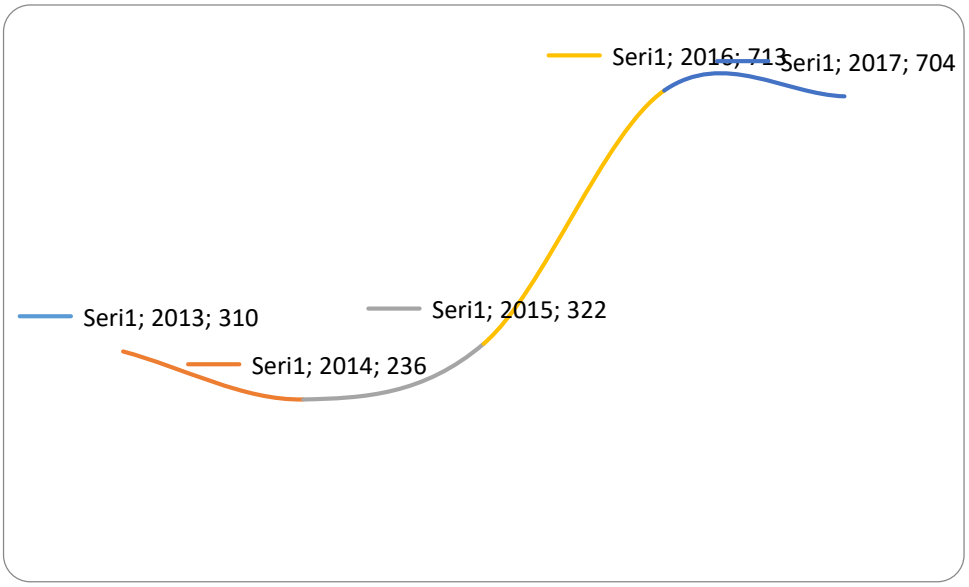
[54] Zvezdan Radojković, Zdravko Skakavac, 'Current Trends in High Tech Crime in the Republic of Serbia, 16 (2019) CP 2017, 222



Source: Radojković, Skakavac n53

In addition to working directly on detecting, clarifying and proving cybercrime, the HT Police also acts as a contact point in accordance with the aforementioned Convention on Cybercrime, and cooperates with other authorities, both nationally and internationally. What is particularly characteristic of this HT Police is that the High-Tech Law defines that it should act on the requirements of the Special Prosecutor's Office, which has an inherent competence in the field of combating cybercrime. In order to look at the activity of the HT Police in the fight against cybercrime, we will use the empirical aforementioned research. In 2013-2017, the Serbian police detected and reported a total of 3,824 cybercrimes (broadly sense), of which 91 were cybercrime (in the narrower sense), which was only 2.4%, 328 for intellectual property criminal offenses (8.6%), as well as 3,405 other criminal offenses (related to pornography, payment cards, forgery, trade secret, etc.), which is 89% (Chart 5).

Chart 5 – The activity of HT Police



Source: Radojković, Skakavac n53

As can be seen only in the five-year period, the number of activities of the HT Police increased twice as much, while in 2016 it was the most critical. Such an increase in the number of activities should also accompany the expansion of the service, especially in terms of human resources and spatial working conditions. We believe that the specialized authorities of the Republic of Serbia

have relatively good human and material resources to combat this extremely dangerous form of crime, where criminal informatics and forensics have a special place in order to obtain relevant evidence for prosecuting perpetrators and criminal offenses.

CONCLUSION

Countries seeking to join the EU and the harmonization of national legislation in the field of cybercrime must be adapted to the definitions of certain terms used in the field of cybercrime, then agree on certain legal institutions, criminal offenses, criminal and other sanctions, etc.

In criminal sense cybercrime means criminal offenses against the security of computer data, while in functional sense it means a High-Tech crime which includes all those criminal offenses where information technologies occur with the object or means of execution and with high material damage, or if the modus operandi indicates the cybercrime (e.g., intellectual property offenses related to pornography, payment cards, and related offenses).

All criminal offenses are issued in material criminal legislation in a separate section of the CC (or CL). Criminal sanctions for cybercrimes range from a fine or imprisonment till three months as the mildest, to imprisonment of up to ten years as the most severe sentence. Seizure of items as a security measure shall be made compulsory in relation to the devices and means of the criminal offense (personal computer, laptop, and equipment) provided that for certain criminal offenses the condition is that the items are the property of the perpetrator. With the exception of one criminal offense for which prosecution is initiated in a private lawsuit, all other criminal offenses are prosecuted ex officio. The material criminal legislation in Serbia can be judged to be largely in line with the EU legal framework, with the exception of one criminal offense prosecuted in a private lawsuit, which from the aspect of international cooperation in this area, the use of specific evidentiary measures and activities on detection and proving of that crime may be disputed.

The role of the police and public prosecutor in detecting, clarifying and proving cybercrime is primary. Considering procedural legislation, these bodies have sufficient procedural capacity to successfully combat this type of crime. These include operative-pursuit, general and special evidentiary measures. Most cybercrime evidentiary measures are conducted only upon the order of a pre-trial judge. In the process of gathering evidence, the most important thing is to respect all the specifics of cybercrime and the principles of legality, authenticity and relevancy.

Comparative legal observing the material criminal law of some countries from the former Yugoslavia, we conclude that the offenses of cybercrime (narrowed sense) are issued in special part of Criminal Law/Code, and that criminal sanctions against the type of relatively the same until the severity vary. The prosecution of cybercrime offenses is executed ex officio with the exception of Republic of Srpska (BIH) where prosecution is executed for one criminal offense on the proposal of the victim. The number of cybercrime offenses is not the same. Republic of Srpska (7), FBIH (6) and Montenegro (6) where, for example, there is no computer sabotage but essential enforcement actions exist in other offenses. The criminal sanctions are the same in type – fine, imprisonment and confiscation of items. Criminal legislation of Montenegro and FBIH issues the most severe sentence of 12 years in prison.

Empirical research shows an increase in the activities of Serbian law enforcement agencies in the fight against cybercrime, understood in broadly sense. On the other hand fewer cybercrime cases end up in court and even fewer ends up in prison. This also shows us that in the area of cybercrime in Serbia there is a phenomenon of ‘criminal funnel’.

In the coming period, all Western Balkan countries, including Serbia, must put more effort into reforming the criminal legislation, and in particular the reform of the judiciary. In addition,

constant education of all cybercrime officers must be ensured through training and professional development programs at educational institutions in Western Europe and the USA.

THE ARTIFICIAL INTELLIGENCE – AN ACTUAL ”GAME CHANGER” IN THE ADMINISTRATION OF CRIMINAL JUSTICE

Associate professor Cristian Dumitru Miheș
Director of Law and Administrative Sciences Departament
Faculty of Law – University of Oradea (Romania)

Abstract

The technical progress is obvious and, consequently, felt in all areas of social life. From our point of view, the return to the previous stage is impossible, except for the intervention of a social cataclysm. As such, the Law Science must deal, in its turn, with the issues arising from the use of more advanced forms of information technology. Often the Law reacted only to a social change or intervention, by norms, by practice or by doctrine. The ideal situation would be even a degree of anticipation, at least in the sense of anticipating debates about future problems and phenomena.

An increasing concern of the legal environment is that of the influence and effects of advanced technology at the social level, especially within the Law. It can hardly be excluded today from the use of advanced forms of software and applications in working procedures that are basically the way of functioning of legal entities, whether governed by public law or by private law. In this context, we can look at the issue of information technology related to criminal law from a number of perspectives: from the perspective of the administration of justice, from the perspective of the one who investigates an criminal offence as provided by penal law, and from the perspective of the person who uses or is ... a form of artificial intelligence.

European Commission for the Efficiency of the Justice (CEPEJ) adopted in December 2018 ”The European Ethical Charter on use of Artificial Intelligence in judicial systems and their environment”. The CEPEJ Ethical Charter does include 5 basic principles: principle of respect of human rights, principle of non-discrimination, principle of quality and security, principle of transparency, impartiality and fairness and principle of user`s control. Starting from the question - Is this European Ethical Charter a sufficient and effective instrument to guide the national legislators to approach and address the problem of Artificial Intelligence as a ”game changer[1]*” in the administration of criminal justice? - the paper will try to underline how the 5 principles mentioned above can be integrated in legislation and in the process of justice administration, especially criminal justice. Also, we would like to offer our opinion of the factual impact of these principles within the criminal justice of our country.*

Furthermore, if we are looking at practical elements - cybercrimes have specific features that differentiate it from other "traditional" crimes. Therefore, a response from the judicial authorities to counteract this phenomenon can only be drawn from the understanding of how the phenomenon manifests itself. In this respect, it has been shown that the phenomenon of cybercrime

[1] Addressing the challenges created by AI to human rights, democracy and the rule of law, The Council of Europe organized a high-level conference under the theme: *"Governing the Game Changer - Impacts of artificial intelligence development on human rights, democracy and the rule of law"*. in Helsinki on 26 and 27 February 2019

needs to be deeply analysed in order to correctly perceive its "psychosocial springs" as well as the objective and subjective factors that "accompany it".

As such, the endeavour of developing new methods of criminal investigation using new technologies, in particular, using more and more different forms of artificial intelligence is just starting. There is no mistake - we are now at dawn of this journey and the road ahead is very, very long.

Also, the challenges of this journey are important, and the solution to those dares is essential for the future effectiveness of criminal investigation. The new methods will have to combine the need for security both at social and individual level, expected as such from the government and, on the other side – the protection of human rights and liberties.

Short summary of the paper

I. Introduction & Hypothesis

- The robots of the '80s generally worked on a fixed algorithm. They could not manage unexpected situations, such as a faulty screw that does not fit, or a broken-down component or when an unexpected (unprogrammed) circumstance did occur (ex. sudden moisture within a sealed dry compartment) etc. Limited computing power and the limits of the sensors affect the productivity because such situations always interfere with any production process based on the famous "assembly line". Instead, however poorly trained, people are easily aware of this kind of problem and "can make common sense decisions."
- C - T thesis (1936): Computable functions are exactly the recursive functions; A function is computable if there is an algorithm that provides its output given its input; The Universal Turing Machine is a "physical,, model of computability; All computers (and hence AI systems) are based on UTM
- Birth of AI : The Dartmouth College Project – 1956 : "The study is to proceed on the basis of the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it. " "An attempt will be made to find how to make machines use language, form abstractions and concepts, solve kinds of problems now reserved for humans, and improve themselves."

- Nowadays, early stages of using some form of artificial intelligence can be found in industrial robots, home robots, the latest in the robots that assist people with reduced mobility or special needs (elderly, disabled) and in the most spectacular of cars without driver.
- Of course, all these developments that were "open to society" are, practically the result of some years of research, especially in the field of military applications (see airplanes without pilot or drones in this regard).
- Decision Delegation to AI systems: AI is used in applications critical to human rights and human well - being: transportation, health, justice, security, warfare, opinion influence, insurance, finance, recruitment, management, personal service, assistance, ...
- Issues: Bias and fairness in data : gender, minorities; Machine decisions are not contextual, lack semantics; Autonomy and Learning challenge reliability, safety, integrity; Algorithms and computational processes are designed by humans; Machines do not grasp the semantics, reasons and foundations of their decisions and actions.
- The responsibility is with the human designers/developers/producers. In case of AI/IS/Robots: Autonomos vs. Independent / Engineers vs. Lawyers (Not the very same concepts/definitions)

- An area in which the intervention of IT technologies is increasing is the justice and law enforcement field dispute is increasingly fierce is that of justice. In a world where formality and bureaucracy - even specific to judicial activities is increasingly standardized - the role of the human factor in the administration of justice decreases every day.
- Databases, person and object recognition programs, simulated behaviour detection tools have replaced the sharp eye or the flair or the investigator's experience.
- Judicial proceedings are carried out increasingly in written with "ticks" on some checklist. The testing and the recruiting of magistrates and lawyers is conducted using multiple choice test.
- And, in the last time, specialized software did enforce certain sanctions. The easiest example is sanctioning of using national and European roads without paying the road tax - where filming on the surveillance camera generates the minutes of sanctioning. If we take into consideration the fact that not very long ago that document was not even signed by a person[2].
- Furthermore, it seems that there is also specialized software designed to assist the judge in solving the case. These software does not only help the court in documenting for the case, but for passing the sentence itself, based on a risk assessment[3]. On the other hand, there are opinions that "a computer program used to calculate sentencing is less accurate and more racist than random humans assigned to the same task" [4].
- All the above, but not only, constitutes the elements of a more accurate picture of the advantages and dangers of using the information technology.

II. Solutions & European response

- Can Machines make Ethical Decisions?
- Need for ethical design and for governance framework & Establishing trustworthy AI
- ***European Union:*** *High-Level Expert Group on AI; AI Alliance; Proposal for Civil Law Rules on Robotics*
- *EU - Ethics guidelines for trustworthy AI. According to the guidelines, trustworthy AI should be: (1) lawful - respecting all applicable laws and regulations; (2) ethical - respecting*

---

[2] In Romania was necessary for the High Court of Cassation and Justice to intervene and to rule that if the document is not signed then it has no power to enforce sanctions – Decision No. 6 from 16th February 2015. However, the decision allows the authority to use electronic signature.

[3] *Stephen Crowley/The New York Times,* **Sent to Prison by a Software Program's Secret Algorithms - https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html *(accessed on 21th of October 2018);*** *The Guardian,* **Artificial intelligence 'judge' developed by UCL computer scientists, https://www.theguardian.com/technology/2016/oct/24/artificial-intelligence-judge-university-college-london-computer-scientists *(accessed on 21th of October 2018);*** *Jason Tashea,* **Courts Are Using AI to Sentence Criminals. That Must Stop Now - https://www.wired.com/2017/04/courts-using-ai-sentence-criminals-must-stop-now/ *(accessed on 21th of October 2018);***

[4] **Julia Dressel, Hany Farid**, *"The accuracy, fairness, and limits of predicting recidivism" (*Science Advances, 17 Jan 2018: Vol. 4, no. 1, eaao5580, DOI: 10.1126/sciadv.aao5580) (http://advances.sciencemag.org/content/advances/4/1/eaao5580.full.pdf (accessed on 20th of October 2018): "Algorithms for predicting recidivism are commonly used to assess a criminal defendant's likelihood of committing a crime. These predictions are used in pretrial, parole, and sentencing decisions".

For example, there was a court case (Wisconsin vs. Loomis) finalized with a six-year sentence, based on such software assessment. The person was arrested in 2013, and he pled guilty to attempting to flee a police officer, and no contest to driving a vehicle without its owner's permission. Although, neither of the offences committed was a violent one, the report on him state as having "a high risk of violence, high risk of recidivism, high pretrial risk." The men "was sentenced to six years in prison based on the finding" - **Kelly Weill**, "*BLIND JUSTICE - Computer Program That Calculates Prison Sentences Is Even More Racist Than Humans, Study Finds*", (https://www.thedailybeast.com/computer-program-that-calculates-prison-sentences-iseven-more-racist-than-humans-study-fin, accessed on 21th of October 2018).

ethical principles and values; (3) robust - both from a technical perspective while taking into account its social environment

• **Council of Europe** : Cyber Crime Convention (2001); Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes; Draft study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework; Draft recommendation on human rights impacts of algorithmic systems 2019;

• Presentation the conclusions of the High Level Conference "Governing the Game Changer – Impacts of artificial intelligence development on human rights, democracy and the rule of law" (Helsinki, 26-27 February 2019)

• European Commission for the Efficiency of the Justice (CEPEJ) adopted in December 2018 "The European Ethical Charter on use of Artificial Intelligence in judicial systems and their environment".

• The CEPEJ Ethical Charter does include 5 basic principles: principle of respect of human rights, principle of non-discrimination, principle of quality and security, principle of transparency, impartiality and fairness and principle of user`s control.

• Starting from the question - Is this European Ethical Charter a sufficient and effective instrument to guide the national legislators to approach and address the problem of Artificial Intelligence as a "game changer[5]" in the administration of criminal justice? - the paper will try to underline how the 5 principles mentioned above can be integrated in legislation and in the process of justice administration, especially criminal justice.

• In direct relation to the administration of justice we can identify the following issues: The responsibility of the decision maker – The IT Tool used must remain an auxiliary of the decision; Transparency in making such a decision [6]; The relationship between the use of information technology and respect for human rights.

• In the same line of thoughts, some authors even speak of a new human right, specific to the digital age: the right not to be judged by a machine entity [7]. We share this view, because otherwise it would come to the situation where decisions about people are made by cars. This view is in line with point 10 of the second thesis of the conclusions[8] mentioned above, which are in the sense that: "AI instruments can support trained judges, while the content and outlines of the laws and legal systems of democratic societies must remain governed. authoritative by people".

• So, the first and last word in decision making must belong to man.

III. Effects & practical aspects:

• Introducing this section, we would like to offer our opinion of the factual impact of these principles within the criminal justice of our country.

• The main problems with the investigation of cybercrime have been synthesized in the literature as follows: identification of the author of cybercrime - perhaps it should be listed at first, but in the vast majority of cases, the author is identified after solving the indicated problems; computer techniques that were used or intended to commit the crime. These objects are sources

[5] Addressing the challenges created by AI to human rights, democracy and the rule of law, The Council of Europe organized a high-level conference under the theme: *"Governing the Game Changer - Impacts of artificial intelligence development on human rights, democracy and the rule of law"*. in Helsinki on 26 and 27 February 2019

[6] în sensul asigurării transparenței și a regulilor de etică, rugăm a se vedea: Paul Bremner, Louise A. Dennis, Michael Fisher, Alan F. Winfield, *"On Proactive, Transparent, and Verifiable Ethical Reasoning for Robots"*, Proceedings of the IEEE, Volume: 107 , Issue: 3 , March 2019, p. 541 – 561, disponibil la: https://ieeexplore.ieee.org/document/8648363/authors#authors

[7] **Silvia Signorato**, *Indagini penali digitali e tutela dei diritti fondamentali, Profili strutturali di una metamorfosi investigativa*, G. Giappichelli Editore - Torino, 2018, p. 101-102;

[8] Conclusions of the Conference *"Governing the Game Changer - Impacts of artificial intelligence development on human rights, democracy and the rule of law"*. in Helsinki on 26 and 27 February 2019

of information for the investigator, a true "source of evidence"; identification of information - obtained after committing cybercrime. In these cases, it is mainly data and information obtained illegally or that should be used to commit acts contrary to the law; identifying the circumstances - which favoured the commission of the crime. In most cases, it is about not providing a minimum of data protection and information systems protection, or the complicity of some people who know the security measures implemented to protect IT systems

III.1. Childpornography. New methods of conducting criminal investigation in cases of child pornography crimes.

- In this context, one can raise an important question: What about crime investigation? Do the new technologies help as much the perpetrators as the law enforcement bodies?
- The answer is yes, but we must bear in mind that the balance of the advantages does shift from perpetrators to law enforcement bodies and backwards continuously.
- One of the most sensitive areas in criminal law and criminal investigation is child pornography. The crime is one of detestable nature, and the social impact of such criminal acts is enormous. Nevertheless, it is important to underline the fact that although measures were taken at global level[9] since so many years, the phenomenon of child pornography still is very present and active.
- The investigation of these crimes is very sensitive and difficult to be carried out taking into consideration certain factors/elements[10].
- When the criminal offence was perpetrated through computer system and especially on-line were identified the following difficulties in criminal/forensic investigation:

a) The issue of competent jurisdiction over the criminal offence. This problem is attached to every computer crime perpetrated on-line an over at least one state border[11]. From procedural perspective any procedural act carried out without having the competence granted by law is sanctioned with annulment of that particular act, as prescribed by the law[12].

b) The issue of the differences in defining the crimes, according to the legislation of each country[13]. These differences can be easily speculated as a method of formal defence, meanwhile the perpetrator will escape criminal responsibility.

c) Unlimited access to the Internet. Now the Internet is largely accessible, cheaper and more and more vast by its limit. Often, searching through Internet means ”looking for the needle in the haystack”, actually.

d) Servers and databases are ”located” in cloud, while cloud computing is expanding and in the meantime cooperation of judicial authorities with Internet giants is difficult, as scholars and practitioners do point out[14].

---

[9] For example: UN Commission on Human Rights, *Programmes of Action for the Prevention of the Sale of Children, Child Prostitution and Child Pornography and for the Elimination of the Exploitation of Child Labour.*, 5 March 1992, E/CN.4/RES/1992/74, available at: http://www.refworld.org/docid/3b00f24950.html (accessed 21 October 2018)

[10] **Michael Lynch**, presentation at the seminar - ”The Life Cycle of E-Evidence: Handling E-Evidence in Child Sex Abuse Material (Academy of European Law, Trier, 18-20 of February 2018).

[11] **Cristian D. Miheș,** *Infracțiuni informatice* (Computer Crimes), University of Oradea Publishing House, Oradea, 2007, p.19.

[12] **Valentin Mirișan,** *Drept procesual penal* (Criminal Procedure Law) (University of Oradea Publishing House, București, 2011) p. 95.

[13] That is why it was important for us to see the differences in determining the concept of ”child pornography”, as described *supra*.

[14] **Alisdar Gillespie**, presentation at the seminar, ”The Life Cycle of E-Evidence: Handling E-Evidence in Child Sex Abuse Material (Academy of European Law, Trier, 18-20 of February 2018).

e) The perpetrators use encryption keys to protect themselves. Encryption is a rather simple method to prevent identification or to hide files – in this case child pornography files. The problem of revealing the encryption key probably will be a subject of another paper work, since it has so many issues to be debated, concerning right to be silenced, right not to self-incrimination, or the judicial authority power to enforce the uncovering of such encryption key.

f) Many of these acts are carried out within the areas of Internet that are undetectable, more or less. The perpetrator uses search engines that do not keep so many e-traces, or in many cases, the dark side of Internet is the host of the chat rooms where child pornography acts are executed. On the other hand, it is more than obvious that within these e-premises you cannot enter and apprehend the perpetrator, in classical, old fashioned manner.

- In this respect, we draw the attention towards a project that was initiated by an NGO: Terre des Hommes – Netherlands[15]. Terre des Hommes was committed to help the children in Filipins, a country where the child sex phenomenon was present on a large scale. But, fighting child sex proved to be difficult, since the poverty rate in the country was very high, there were families (parents) that encouraged children to go to chat rooms, and, also, there was little cooperation from local law enforcement authorities[16]. In these circumstance, a new approach of the phenomenon was necessary, as a consequence, ”Sweetie” was created[17].
- Mainly, ”Sweetie” is an investigative tool, an advanced software that interacts in chat rooms with sexual offender using a portray of a 10 yeas girl. ”Sweetie” can communicate and actually interact, thanks to the artificial intelligence that functions behind the image of that girl. The idea of using an avatar, a form of artificial intelligence in order to get in touch with the suspects, was a revolutionary one, and it led to creating of the ”Sweetie 2.0”: *”Sweetie is a virtual 10-year-old Filipino girl who is present in dark online chatrooms that are frequented by men looking for webcam sex with minors”*[18].
- But, on the other hand, the legal aspects of using such new technology were studied and certain aspects were underlined[19].
- From the perspective of ECHR jurisprudence related to article 6 of European Convention on Human Rights, ”Sweetie 2.0” can be considered:
  - A challenging agent that lures the suspect?
  - An undercover agent of a judicial body?
  - A recording device that keeps track of communication within the chat room?
- In other line of thoughts, ”Sweetie 2.0” can provide information about: the behaviour of people in the "chat-room"; some other aspects recorded while interacting with the other persons in the chat rooms, even about other actual victims; technical data of the computer systems present in the chat rooms.

III.2. Tax evasion

[15] More info about Terre des Hommes – Netherlands can be found at: https://www.terredeshommes.nl/en.

[16] **Hans Guyt**, presentation at the seminar, ”The Life Cycle of E-Evidence: Handling E-Evidence in Child Sex Abuse Material (Academy of European Law, Trier, 18-20 of February 2018).

[17] https://www.savesweetienow.org/; https://www.terredeshommes.nl/en/programmes/sweetie-20-stop-webcam-child-sex (accessed on 21st of October 2018).

[18] https://www.terredeshommes.nl/en/news/sex-date-virtual-minor-now-also-punishable (accessed on 21st of October 2018).

[19] **Bart W. Schermer, Ilina Georgieva, Prof. Dr. Simone van der Hof, Prof. Dr. Bert-Jaap Koops**, *Legal Aspects of Sweetie 2.0*, Leiden/Tilburg, TILT, 2016 : https://pure.uvt.nl/ws/portalfiles/portal/13318907/Sweetie20_report_final_20161003.pdf, see conclusions of the report: p. 82-86 (accessed on 21st of October 2018).

The current and constant evolution of e-technology creates effects in tax evasion, also. This impact is affirmed both in the field of executing tax evasion, and in the field of fraud detection[20]. The present subject, once opened, appears to be extremely large, giving the multidisciplinary implications that it generates. The paper tries to open the floor for discussions and solutions. Therefore, the purpose of this presentation is to point the issue and subject to further analysis – utilization of advanced software or artificial intelligence, in detecting and investigating VAT.

On the other hand, the intervention of the IT technology in our society is a continuous, progressive process. Neither the technology, either the rules and social perception stays the same, but they evolve. Presently, the problem seems to be more ”Cyber” than ”Law” at this point. Since the ”Cyber” area is updating exponentially, then the ”Law” should respond in a very similar manner, in order to keep up with the social evolution.

One of the challenges will be to regulate the activity and effect of software, machines, automobiles or any other devices that use more developed forms of computer programmes. Probably, the essential problem in this respect would be to have concordance between the material and social progress.

An overall look on the phenomenon tax fraud, with glance to VAT Fraud, can identify certain features that have to be taken into consideration[21]:

- First, tax crime is facilitated by technology, and consequently a technology response is needed, but with respect of law
- Secondly, since practically all of us do have access to the INTERNET, there is the problem of on line transactions and the control over these transaction
- Thirdly, the problem of software used to keep the books (accountant books)
- Fourthly, there is the problem of detecting and investigating tax crimes especially within online environment of tax fraud (VAT included)
- Finally, can we talk about on-line fiscal inspection? Could it be possible?

Advanced software and artificial intelligence is changing taxation and, also, tax crimes. Artificial intelligence is just taking its first steps into the meticulous and complex world of taxation[22].

What are disadvantages of human work? They can be structured as[23]:

- *Unreliability – Two people using the same data can reach different conclusions.*
- *Slowness – Humans can consider only one decision at a time, often tediously.*
- *Inaccuracy – Many factors can interfere with positive learned behaviour by humans such as emotions, illness, and fatigue.*

In the meantime, advanced software and artificial intelligence computer algorithms are[24] *transparent, and their detailed function can be understood; they have superior speed, consistent results, never fall asleep (well, sometimes they crash), or have "bad days".*

Many AI approaches are recognizable because they add the word "deep" to their name, such as Deep Learning, Deep Search, Deep Query, and Deep Reinforcement.

---

[20] **Marija Vuković** – ”Towards The Digitization of Tax Administration”, p.1, available at: https://www.cef-see.org/files/Digitization_Tax_Administration.pdf; **Diana Cîrmaciu**, *Public Finance Law*, University of Oradea Publishing House, 2010, pp.115-117

[21] OECD Report, p. 7

[22] **Marija Vuković** - ”Towards The Digitization of Tax Administration”, p. 5, https://www.cef-see.org/files/Digitization_Tax_Administration.pdf

[23] **Cas Milner, Bjarne Berg** – ”Tax Analytics Artificial Intelligence And Machine Learning–Level 5”, p. 6, available at: https://www.pwc.no/no/publikasjoner/Digitalisering/artificial-intelligence-and-machine-learning-final1.pdf

[24] **Cas Milner, Bjarne Berg** – ”Tax Analytics Artificial Intelligence and Machine Learning–Level 5”, p. 6, available at: https://www.pwc.no/no/publikasjoner/Digitalisering/artificial-intelligence-and-machine-learning-final1.pdf

As this trend accelerates, watch for AI to become an increasingly crucial part of progressive - and successful - tax departments. But, will AI/IS uphold the LAW in any time???

What if ... We will replace accountants and tax officers, as there are models to replace lawyers?

If the algoritms are clear, the advanced software is created and implemented, and if the AI could take decisions (independently), then different levels of activity will be replaced:

- ✓ First.... Basic/primary accountancy
- ✓ Then... Financial statements and reports
- ✓ Meatime forecasting, clasification or clustering is more effective even now when it is carried out by advanced software

Further more.... in certain situations, these systems (AI/IS) can be considered as active subjects of a tax crime[25]. The answer cannot be given in a few closing words, as it is debated intensively also in our country.

IV. Concluding, the role of AI or other forms of advanced software in administration of justice, is growing as the role of e-technology will increase in everyday life, so a balanced and effective response from theory and practice of Law is needed.

(as I am to take part in a ERA Seminar in October on this topic – "AI and Criminal Justice", this paper will be improved with "fresh" consideration after attending thist seminar)

[25] ***M.A. Hotca,*** *moderator of the debate* "Artificial Intelligence between Technological Desires and Legal Realities", *(25.06.2018), as well as other views, all available at http://htcp.eu/?s=artificial (accessed 12.03. 2019);* ***L. Stănilă***, "Artificial Intelligence: A Challenge for Criminal Law", *in the Romanian Journal of Business Criminal Law, Nr. 2/2018;* ***Adrian Sandru,*** "Artificial Intelligence. Installation of Computer Algorithms in the Field of Criminal Law" *available at: https://www.juridice.ro/587545/intelligence-artificial-install-information-algorithms-in-the-domain-penal.html (accessed 12.03.2019); 2019;* ***C. Miheş****, "*Man-computer interaction. Legal Implications " *in the Journal of the Faculty of Law Oradea, Nr. 1/2018, "ProUniveristaria" Publishing House, Bucharest, 2018;*

Updating Cyberjustice Data in Brazil: Moving Forward with Artificial Intelligence.

Fausto Martin De Sanctis - Federal Appeals Judge in Sao Paulo, Brazil

I. Introduction.

Brazil had 80.1 million cases pending at the end of 2017 (79.7 million at the end of 2016; Supreme Court: 43,283 lawsuits in process (originating and appeals) on 28.08.2018.[1] Besides public direct access to hearings, live sessions from Supreme Court have TV Coverage.

Besides, in order to improve the day-to-day functioning, transparency, and quality of the justice system, Brazil is making available to the beneficiaries of Justice, what we call Itinerant Justice, as well as TV Coverage of Hearings, Home Office or Work At Home, the National Database of Arrest Warrants – BNMP 2.0, Digital Lawsuits, and Artificial Intelligence.

The main goal of these tools leads to an increased capacity of the judicial delivery to beneficiaries, which is able to assess the efficiency of the Brazilian judicial system, ensuring that justice is delivered within a reasonable time and that it meets good quality standards.

There are some inbuilt flexibility in thinking about efficiency and the need to deliver justice and mitigate the risk of obsolescence of some formalities.

The reason for this work is to show how Brazil has been treating the subject of efficiency of Justice in the face of large numbers of cases and the application of new technologies.

II. Itinerant or Traveling Courts.

The Itinerant Court of the Court of Justice of the State of São Paulo consists of two trailers, which visit neighborhoods of the city with pre-established addresses facilitating the population's access to justice. One vehicle is used to make the call and the other returns to the location about a month later to hold the scheduled hearings. The itinerant has existed since August 1998 and has the same jurisdiction as the special civil courts, that is, attends causes of up to 40 minimum wages, and there is no need, for causes of up to 20 wages, to hire a lawyer. Trailers are equipped with notebooks, printers and playback machines.

The itinerant's most frequent issues are consumer law, health insurance, general charges, neighborhood conflicts and traffic accidents. The system does not accept labor claims.[2]

---

[1] See CNJ site, *Justiça em Números*, *in* http://www.cnj.jus.br/mwg-internal/de5fs23hu73ds/progress?id=02BblvxN38kXtXRYmmPZ6vmOT6QiI7qBOA_BxsQ-tFs, accessed on Dec. 15, 2018.

[2] Anyone over 18 years of age with Identification Number (RG) may search for care and file an action. It is important to provide the name and address of the defendant. Private companies, disabled people, prisoners, public companies of the Federal Government, bankruptcy cases and insolvent citizens may not be parties to these proceedings. The plaintiff reports the case and the clerk summarizes it. If the applicant's domicile is in the same region of the service, a conciliation hearing will be held, carried out in the average term of one month, when the itinerant trailer returns to the place and will continue until the judgment of the case at the Office of the Permanent Traveling Court. Otherwise, the records are sent to the trial court for processing and judgment of the case. If there is an injunction request, the case is immediately referred to the judge for consideration and then referred to a trial court. The service is free (see State Appeals Court of Sao Paulo site, *Justiça itinerante*. *In* http://www.tjsp.jus.br/Especialidade/Itinerante, accessed on Aug 14, 2018).

On the other hand, judges and servants from the Northern Region of the country travel for hours on boats or airplanes to bring to the riverbank population access to justice. Some of these places are accessible only by planes or boats. Across the Amazon River and through the Amazon jungle, Judiciary teams serve thousands of people living in communities with the worst Human Development Indexes (HDI) in the country - such as the Bailique archipelago in Amapá State or Jordão in Acre State. In all these expeditions, the Justice acts far beyond the processes: it promotes actions of basic citizenship and prevention of conflicts.

For the Council member to the National Council of Justice (CNJ) Daldice Santana, president of the Commission on Access to Justice and Citizenship of the body, it is not rare that it can be identified that the population is needier where there is more physical detachment from the Judiciary and other public services.

"The natural would be the presence of the judge and other servants where there are more people in need, but this does not happen, because several of them do not even know they have the right, even more they can exercise it. In this way, demand for public services is not generated, which causes the statistical maps to point to a false impression of satisfaction of rights", says Daldice Santana.[3]



III. Home Office or Work at Home.

Due to important initiatives, the National Justice Council (CNJ) has issued the regulation of Work at Home system by staff from Courts. It is possible for up to 50% of the civil servants to work from home drafting solutions of some cases.[4] They have remote access justice facilities.

---

[3] See National Council of Justice – CNJ site, *Justiça Itinerante: juízes vão até os ribeirinhos da Amazônia*, *in* http://www.cnj.jus.br/noticias/cnj/85037-justica-itinerante-juizes-vao-ata-os-ribeirinhos-da-amazonia, accessed on Dec. 15, 2018.

[4] Resolution CNJ n.º 227, Jun. 15, 2016.

This has been implemented little by little throughout the country.

IV. The National Database of Arrest Warrants – BNMP 2.0.

The National Database of Arrest Warrants – BNMP was implemented by CNJ in 2011 and in 2018 a new version integrated all courts all over the country. It is a digital tool that allows the recording and consultation of information about arrest warrants.

The overcrowding of prisoners made worse the crisis inside the prison system and have shown the need for broader data and reliable information to enable planning a change of this reality in Brazil.

The CNJ developed the BNMP 2.0 as a National Prison Monitoring Database System, allowing, in addition, the monitoring of arrest warrants issued by the Judiciary, controlling the execution of the arrest and release judicial orders in a national scope and in real time. With this tool, it has allowed the creation of a National Registry of Prisoners.

The Register brings more security to society and efficiency for the Judiciary, since all information about wanted people by the judicial system or arrested prisoners in different states is now integrated.

There is now a dynamic and national database.[5]

V. Inherent benefits of the Adoption of Digital Lawsuits.

In short, many parties might believe "outsourcing" judicial services to be an overwhelming exercise. However, in fact there are many advantages to the digital/electronic processes making it more or equally efficient than other methods of conflict resolutions, well established to improve justice delivery, like mediation and arbitration:

a) Productivity Increase – Digital processes allow for 24/7 works with fewer civil servants working on repetitive and time consuming tasks; it has been observed un increase of cases in trial courts using the PJe;

b) Reduced Financial and Environmental Costs – A physical procedure cost is high. The digital processes cause the improvement of the environment due to the economy of the necessary inputs for the production of paper (cutting of trees, consumption of water, use of chemical products, and consumption of energy). It is estimated that 100,000 electronic processes generate a saving of 34 million of sheets of paper (in addition to covers, labels, boxes, staples and printing ink), which means the preservation of 1,700 trees. Today the court has approximately 2 million and 500 thousand processes, equivalent to 833 million sheets of paper or 41,650 trees; 100 million of cases represent less 34 billion of sheets of paper and the preservation of 1,700,000 trees. [6]

---

[5] National Council of Justice – CNJ site, *Cadastro Nacional de Presos - BNMP 2.0*, http://www.cnj.jus.br/sistema-carcerario-e-execucao-penal/cadastro-nacional-de-presos-bnmp-2-0, accessed on Dec. 15, 2018.

[6] According to the Advisory for Integrated Development and Strategic Management Department of the TRF3.

c) Faster and Precise Data Collection and Risk Assessments – Process automation allows exact statistic data and assessments with lesser human time and effort;

d) Accuracy – the digital processes are able to self-learn and be taught to handle exceptions since machine recognizes and analyses judicial jurisprudence trends quickly, which in turn allows for instant detection of misinterpretation or alerts; this system also perform behavior modeling which increases the accuracy of standardization of proceedings;

e) Increased Judicial Confidence – If the system works in a better way, qualitatively and quantitatively, this means that the Judiciary is not failing to recognize the problems of the people what it would be the first step to losing people's confidence, and legitimacy.

In the opposite direction of the debates on the subject, the Brazilian Congress is trying to create more federal courts of appeals instead of rethinking the whole judicial system against technological revolution and the benefits of an online court system.[7]

VI. Digital Lawsuits

The Civil Procedure Code, Law n.º 13,105, 16 March 2015, states that "Procedural acts may be totally or partially digital, so that they can be produced, communicated, stored and validated electronically, in accordance with the law" (article 193), and that "Procedural automation systems shall respect the publicity of the acts, access and participation of the parties and their attorneys, including in the hearings and trial sessions, observing the guarantees of availability, independence of the computing platform, accessibility and interoperability of systems, services, data and information that the Judiciary Administration manages in the exercise of its functions" (article 194).

With the support of the CNJ and after some initiatives of good practices which enabled the successful development and implementation of information and communication technologies in the Judiciary branch, electronic processes have been implemented nationwide since 2013. It is called PJe (Electronic Judicial Process).[8] This initiative contributes to understanding how to ensure a successful change towards Cyberjustice in Brazil. In São Paulo, which has the highest number of cases in Brazil (about 55%), it was fully implemented at the end of 2018 (exceptionally for criminal cases and tax decision's enforcements).[9]

The Electronic Judicial Process does not require the use of paper, avoids the displacement of the parties to the protocol of their petitions and documents and reduces the risk of damages and mistakes In addition, the system expedites the remittance of processes to the

[7] Constitutional Amendment n.º 73/2013 not yet adopted (creation of Federal Appeal Courts in the capitals of Curitiba, Belo Horizonte, Salvador e Manaus, respectively the states of Paraná, Minas Gerais, Bahia and Amazonas).
[8] Resolution CNJ n.º 185, Dec. 18, 2013.
[9] Electronic Judicial Process (PJe) arrived at the Federal Courts of Mato Grosso Sul State and reached the entire 3rd Region which covers the states of São Paulo (SP) and Mato Grosso do Sul. Changing the view of procedural acts in the digital environment requires less user time and makes PJe simpler to operate with fewer clicks and a more intuitive interface. The new Version 2.0 also facilitates the insertion of reminders in the processes and the visualization of the tasks, besides allowing the use of different browsers (Resolution from the Federal Court of Appeals for the Third Region – TRF3 n.º 88, Jan. 1st, 2017).

second degree, in case of appeal, saving shipping costs and return that are charged only on physical processes.

Other advantages of the PJe are the elimination of bureaucratic tasks such as the gathering of petitions and proceedings, the release of physical space and the faster obtaining of information and certificates. In short, the system facilitates the processing of cases and rationalizes costs, allowing the use of financial costs and personnel in activities more directed to the purpose of the Judiciary: resolving conflicts. These resources are transferred from bureaucratic tasks to the analysis of the evidence and arguments of the parties.

In this way, the electronic process will allow the reduction in the processing time of the processes. There will be improvements in trial sessions, process visualization and use of electronic signature. Also for the near future there will be the interoperability of the PJe and the system of state courts of justice. With this, the referral of processes that process by delegated competence will be done electronically for Federal Court of Appeals for the Third Region (TRF3). Another important step towards modernization, the TRF3 will no longer receive physical appeals.

The CNJ provides PJe Browser application, which is a specific version developed for the user of PJe installed in the courts.

The current Chief Justice of the Brazilian Supreme Court (STF) and the National Justice Council (CNJ), Justice Dias Toffoli, and the President of the Federal Court of Appeals for the 3rd Region (TRF3), Federal Appeals Judge Therezinha Cazerta, in November 9th, 2018, officially launched project "TRF3 100% PJe", whose goal is to insert all lawsuits in the Federal Court of the 3rd Region in the environment of the Electronic Judicial Process (Pje).[10]

Since August 2017, all civil proceedings - with the exception of tax foreclosures - that have been filed in the Federal Trial Courts of the States of São Paulo and Mato Grosso do Sul have already been initiated in the PJe, a system for processing judicial proceedings prepared by the CNJ, which allows the practice of all acts electronically - from the proposition of the action to its filing. In October 2018, the number of electronic processes reached 500 thousand.

However, a large liability of actions prior to the implantation of the PJe remains in physical environment. Thanks to a partnership between the TRF3 and the CNJ, part of this collection that is still processed on paper began to be virtualized and inserted into the electronic system.

In this first stage, the support of the CNJ allowed the hiring of a specialized company had digitized and inserted in the PJe civil and social security lawsuits that were in paper in the Social Security Trial Court of the Federal Judiciary in the capital of São Paulo and in ten other ones - Americana, Bragança Paulista, Campinas, Limeira, Jundiaí, Mauá, Registro, Santos, São João da Boa Vista and São Vicente. The works lasted about 40 days, with a scanning of 21.1 million pages, equivalent to 44,749 lawsuits. The figures represent, for the Judiciary Section of São Paulo, 51.13% of its social security and 13.3% of the civil collection.

Besides it, at the Federal Court of Appeals for the Third Region (TRF3) part of the sessions are made electronically in case of no request of oral arguments from the parties. Also, parties can make their oral arguments by videoconferencing.

---

[10] ClippingOnline, TRF3, *TRF3 100% PJe: PRESIDENTES DO CNJ E DO TRF3 LANÇAM PROJETO PARA REDUÇÃO E VIRTUALIZAÇÃO DO ACERVO DE PROCESSOS FÍSICOS DA JUSTIÇA FEDERAL DA 3.ª REGIÃO. Na primeira etapa, processos que tramitam em papel em 11 Subseções Judiciárias do Estado de São Paulo serão inseridos no PJe até o final de 2018.* http://web.trf3.jus.br/noticias/ClippingOnline/Noticia/Exibir/374929, published on Nov. 12, 2018, accessed on Dec. 15, 2018.

VII. E-Courts: Overcoming Budgetary Guidelines.

The director of the Forum of the Judiciary Section of São Paulo, Federal Judge Luciana Ortiz presented another project related to the virtualization of lawsuits in the Federal Trial Courts in the 3rd Region: E-Court, a new organizational model that adjusts the structures of the Federal Trial Courts to the resulting reality of the Electronic Judicial Process (PJe).

With the goal of strengthening the support structure for the jurisdictional activity, the proposal is to share the infrastructure and human resources of the Federal Trial Courts, through the creation of specialized centers in the execution of standardized tasks. For this, it is necessary a high degree of scanning of the lawsuits.[11]

In terms of budgetary situation of the Federal Justice, it is on the same stance as in 2016 because of the amendment that came out (Constitutional Amendment 95/2016) which froze public spending for 20 years.

The direct consequence of this restriction was the shrinkage of the 3rd Region Federal Justice System. Since aforementioned Amendment, the Federal Appeals Court has failed to fill vacancies opened by retirements or deaths, once the payment of the pension in these cases comes from the budget of the court. So, if payments go to pensions, there is no budget for income salary of new civil servants who fulfill vacant positions. In December 2018, there were 485 vacant civil servant positions, besides plus 100 judges. In 2018, only 36 approved servants were nominated from public examinations held in 2013. Twelve positions were assigned to the Federal Appeals Court, 22 to the Judiciary Section of São Paulo and 2 to the Judiciary Section of Mato Grosso do Sul (trial courts in these states).

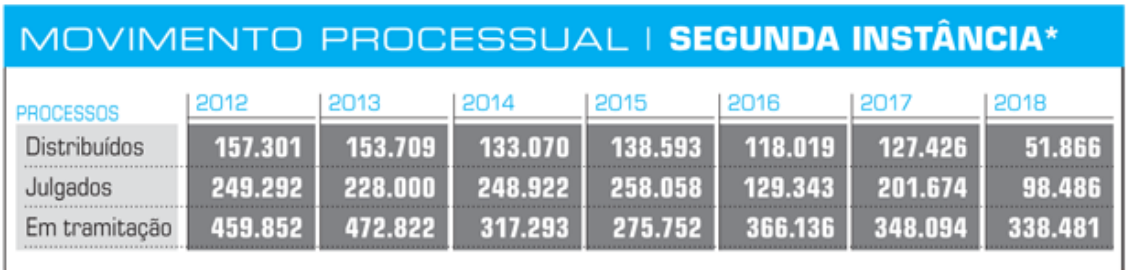
The movement of the lawsuits in the first instance (filed, tried and pending ones):

MOVIMENTO PROCESSUAL | **PRIMEIRA INSTÂNCIA***

PROCESSOS	2012	2013	2014	2015	2016	2017	2018
Distribuídos	487.794	547.528	638.017	601.564	602.138	550.380	257.014
Julgados	422.848	398.023	424.250	433.874	438.952	444.269	356.069
Em tramitação	1.942.605	2.046.620	2.218.101	2.412.322	2.633.453	2.822.762	2.810.733

The movement of the lawsuits in the second instance (filed, tried and pending ones):

[11] ClippingOnline, TRF3, *TRF3 100% PJe: PRESIDENTES DO CNJ E DO TRF3 LANÇAM PROJETO PARA REDUÇÃO E VIRTUALIZAÇÃO DO ACERVO DE PROCESSOS FÍSICOS DA JUSTIÇA FEDERAL DA 3.ª REGIÃO. Na primeira etapa, processos que tramitam em papel em 11 Subseções Judiciárias do Estado de São Paulo serão inseridos no PJe até o final de 2018.* http://web.trf3.jus.br/noticias/ClippingOnline/Noticia/Exibir/374929, published on Nov. 12, 2018, accessed on Dec. 15, 2018.



MOVIMENTO PROCESSUAL | **SEGUNDA INSTÂNCIA***

PROCESSOS	2012	2013	2014	2015	2016	2017	2018
Distribuídos	157.301	153.709	133.070	138.593	118.019	127.426	51.866
Julgados	249.292	228.000	248.922	258.058	129.343	201.674	98.486
Em tramitação	459.852	472.822	317.293	275.752	366.136	348.094	338.481

The 3rd Region is the one that works with the most updated version of the PJe. In 2018, TRF-3 invested 1,262,223 reais (321,995 American dollars)[12] in the development and implementation of the PJe, in accordance with the stipulations of the Budget Guidelines Law. The Federal Appeals Court had only 14 servants working in the development of the flows and in the support (call center) for the internal and external public.

According to the 3rd Region Judge Inspector, Carlos Muta, "in this scenario, of course, the transition tends to be difficult and slower, but it is known that, administratively, the development of the JCe financial resources is - and has been seen - priority of all the management areas of the court, "he says.[13]

Another serious consequence was that the money ended in August 2018, and the amount had to be supplemented by the Executive Branch to cover the current deficit (shortage). To make matters worse, the National Congress had imposed a 26.5% cut in the Federal Justice budget in the 2019 Budgetary Guidelines Law. To overcome this dramatic financial situation, the Federal Appeals Courts are making some decisions addressing changes from idle Courts into high litigation Courts. With the electronic lawsuits, the work needs fewer civil servants.[14]

VIII. Artificial Intelligence Application to Judicial Decisions.

Disciplining the access to the data deposited in the databases of the Brazilian courts and looking for cutting-edge solutions in the management of information technology were the subjects discussed in the panel Artificial Intelligence in the Judiciary, held on Dec. 4, 2018 at the XII National Meeting of Judiciary, in Iguassu Falls (Foz do Iguaçu) in Paraná state.

In the opening panel, the counselor Márcio Schiefler, president of the Permanent Commission for Information Technology and Infrastructure of the National Council of Justice (CNJ), stressed the importance of the Judiciary to take the lead in this area. According to him, "information is power. We live in a country with a highly judicialized life, how much are the information deposited in the court databases?

---

[12] 3.92 in Dec. 17, 2018 (www.dolarhoje.com).

[13] ClippingOnline. Thiago. Crepaldi. In Federal Judiciary Yearbook 2019 (Anuário da Justiça Federal 2019), *launched on Nov. 21, 2018. Teto dos gastos públicos trava investimentos no TRF da 3ª Região*, http://web.trf3.jus.br/noticias/ClippingOnline/Noticia/Exibir/375348, published on Nov. 24, 2018, accessed on Dec. 15, 2018.

[14] ClipplingOnline. Thiago Crepaldi and Damilo vital. *In Justiça Federal será toda remanejada com o processo eletrônico*, http://web.trf3.jus.br/noticias/ClippingOnline/Noticia/Exibir/375142, published on Nov. 16, 2018, accessed on Dec. 17, 2018.

Faced with this scenario, where the private sector offers free services to the courts in exchange for free access to procedural information, the counselor highlighted the need for the CNJ, in cooperation with the courts, to take the lead in this new field.[15]

On the other hand, justices of the Brazilian Supreme Court (STF) obtained an ally for the number of more than 39,000 cases of the Court: the name is Victor and it promises to make decisions in 10 million cases to refer to the lower instances to recognize a topic of general repercussion.[16]

Victor is been considered the twelfth Justice (out of eleven), not even an auxiliary judge in person. Despite the human name, Victor is an artificial intelligence tool, with a cost of R$ 1.6 million (408,163 American dollars)[17], in partnership with the University of Brasilia (UnB), and will be fully deployed until the beginning of 2019.[18]

Victor knows how to interpret resources, separate them by themes and highlight the main pieces to streamline court proceedings and to unlock justice chambers. In some cases, the system already does in 5 seconds the service that employees took more than 30 minutes.

In addition, Victor has the potential to give a solution alone to about one-eighth of the extraordinary appeals (REs) that come to the Supreme Court - as in 2017 80,000 ones were presented to the Court. So, it could have ended 10,000 cases that year if it was already implemented.

Victor will automatically return to the home court extraordinary appeals that fit into one of the 27 hypothesis of general repercussions that the instrument was taught to identify. The return is due both to apply a thesis already approved by the Supreme Court, or to suspend a lawsuit for a final definition of the justices for the case. This function of the tool, however, is still being improved, as it currently has an average accuracy of almost 90%. The court technicians work with UnB to get a smaller margin of mistakes before implementing it, which is scheduled for early 2019.

One Victor service that is already in use is the identification and separation of the five main parts of the case: the judgment under appeal, the judgment on the admissibility of the extraordinary appeal, the petition of the extraordinary appeal, the trial court judgment and a possible subsidiary appeal of it.

The servants of the General Repercussion department used to take 30 minutes to perform this activity. Now the robot does the job in just 5 seconds. In many cases, the department did not even do this division and sent the process to the rapporteur without separation.

---

[15] ClippingOnline from the National Council of Justice – CNJ site. In *CNJ anuncia a criação de laboratório de inteligência artificial para o PJe*, http://web.trf3.jus.br/noticias/ClippingOnline/Noticia/Exibir/375711, published on Dec. 4, 2018, accessed on Dec. 17, 2018.

[16] JOTA site. Matheus Teixeira. *STF investe em inteligência artificial para dar celeridade a processos. Ferramenta Victor identifica se recursos se enquadram em repercussão geral e destaca, em segundos, peças principais*, https://www.jota.info/coberturas-especiais/inova-e-acao/stf-aposta-inteligencia-artificial-celeridade-processos-11122018?utm_source=JOTA+Full+List&utm_campaign=f280786d7c-EMAIL_CAMPAIGN_2017_10_06_COPY_01&utm_medium=email&utm_term=0_5e71fd639b-f280786d7c-380321969, published on Dec. 11, 2018, accessed on Dec. 17, 2018.

[17] 3.92 in Dec. 17, 2018 (www.dolarhoje.com).

[18] The name is a tribute to Victor Nunes Leal, but not only because he is cited today for his legal theses defended as STF justice from 1960 to 1968, when he was removed by the Institutional Act 5 (AI-5) in the dictartoship time.Victor's name was also chosen because the former justice was the first court magistrate to try to systematize the precedents of the court.

Now, after the chambers received the files for the already highlighted pieces, the justices have requested that the same work must be done with the previous cases under their responsibility before Victor, in order to facilitate the elaboration of the decisions.

To select the main pieces, Victor does a previous work that is also seen with very good eyes by advisors who help the justices to prepare their decisions: it transforms text files that are in image form into a format in which it is possible to select snippets to give the famous "ctrl + c, ctrl + v".

Victor goes far beyond searching for key words to identify the hypothesis. It searches the context, associates more than one document in order to get to the identification of that topic. It actually seeks the understanding of the expressions being used together, based on repetition.

Victor will stimulate other courts across the country to invest in artificial intelligence to help expedite justice. It serves as an example for them to develop artificial intelligence tools to help with the work. Before forwarding the cases to the Supreme Court, Courts must already identify whether the case fits into some general repercussion issue, using the new technology in order to optimize efforts and give the appropriate treatment: suspending or applying already signed understanding of the Supreme Court.

In fact, Victor was an initiative of the Brazilian Supreme Court to promote the development of investment in innovation in the judiciary as a whole. Out of 80,000 appeals that reach the Brazilian Supreme Court each year, 40,000 are returned to the courts of origin on average. So, half cases have not formal admissibility requirements and half falls under some general repercussion hypothesis defined by the Supreme Court.

The lawyer who disagrees with the referral given by the tool may, as in other cases, appeal the decision and ask for a re-discussion on the case.

There is a fear of public managers of the legal environment in signing this type of contract. The reason is that it is complex to establish parameters for bidding in the area. It is very difficult to bid artificial intelligence using Bidding Law n.º 8,666, June 21, 1993, for example, because it is difficult to find competitors among companies, making difficult to define which company is better than the other.

Due to the fact that the University of Brasilia is working together in this project, others courts have been more comfortable to advance in artificial intelligence like the Superior Labor Court or Superior Court of Justice.

As in the Supreme Court Victor is restricted to general repercussions, it signed a decentralized execution term, and it was agreed that the university would conduct a survey of how many scholarships it would have to pay - what it needed to make Victor functioning - while the court would reimburse UNB for these expenses.

The Secretary of Information Technology of the Supreme Court, Edmundo Veras, estimates that the Supreme Court has already recovered its investiment and has further extended the Court's economy. "In the first semester, we received 42,000 cases. If we had to do the work of identification of the major parts of them, we would need 22,000 hours of servant work just to separate the documentation. It would take two and a half years to do in all cases, at an approximate cost of R$ 3 million" (765,306 American dollars).

According to him, the process to guide Victor to make the right decisions required hundreds of decisions of the Chief Justice Presidency in which a certain understanding had been applied for general repercussion. There, Victor learned that when it has in a lawsuit coincidence of parts that use use certain terms, the solution given by the Chief Justice was in a certain way.

To define how to use artificial intelligence, there were numerous meetings of the Information Technology Management Committee of the Court. And after the meetings and talks with the Judicial Secretariat and the Chief Justice Presidency, it was concluded that the tool should focus on the issues with general repercussions.[19]

IX. Conclusions.

Having a continental territory with many economic and social diversities, the Brazilian judicial system still strive to reach far-small villages to provide public access and deliver justice.

At the same time, it would say that Brazil is in a step back of the discussion of implementation of new models of justice spaces, still dealing with the deployment of digital lawsuits in a very extensive amount of cases, in other way is using new technologies to face them.

The California Executive Research Court Technology Tour 2017[20] showed that this important initiative made us go into the debate about the need of a deep rethinking of the judicial spaces and system in face of the importance of automation.

Due to the still judicial and cultural entrenched behavior, changing judicial space will require reflections and convincing efforts to show the significant benefits to a more communal judicial working practices by fostering a more collegiate and supportive atmosphere. It is need to refine the overall conception of what a court is taking account of recent developments in technology with raise the possibility of courts and tribunals having virtual manifestations.

In order to improve the day-to-day functioning, transparency, and quality of the justice system, Brazil is made available Itinerant Justice, as well as TV Coverage of Hearings, Home Office or Work At Home, the National Database of Arrest Warrants – BNMP 2.0, Digital Lawsuits, and, in 2018, Artificial Intelligence.

Brazil are facing a new paradigm break, aiming an increased capacity of the judicial delivery to beneficiaries, within a reasonable time, good quality standards, and the use of artificial intelligence.

Its use requires having a very large number of decisions, and Brazil has a lot. From now on, with the beginning of the application of the artificial intelligence on the Brazilian courts, it is possible to predict that civil servants responsible for the traditional work will be able to focus on more qualified activities, not wasting time on those works that can be replaced by technology.

---

[19] JOTA site. Matheus Teixeira. *STF investe em inteligência artificial para dar celeridade a processos. Ferramenta Victor identifica se recursos se enquadram em repercussão geral e destaca, em segundos, peças principais*, https://www.jota.info/coberturas-especiais/inova-e-acao/stf-aposta-inteligencia-artificial-celeridade-processos-11122018?utm_source=JOTA+Full+List&utm_campaign=f280786d7c-EMAIL_CAMPAIGN_2017_10_06_COPY_01&utm_medium=email&utm_term=0_5e71fd639b-f280786d7c-380321969, published on Dec. 11, 2018, accessed on Dec. 17, 2018.

[20] This tour took place from September 18 to 22, 2017, and was supported by an international group of scholars, the Cyberjustice Consortium, from the University of Montreal, the Western Sidney University, the American Institute of Architects' Academy of Architecture for Justice, and the French *Institut des Hautes Études sur la Justice.* The so called project for the Court of the Future Network organized an executive research tour to courts and technology facilities in California, travelling from San Francisco to Los Angeles and visiting three federal and two state courts, and the headquarters of Cisco and Facebook. The tour was attended by lawyers, judges, court officials, architects and those involved in court architecture and design, court security professional, academics and researchers – in Law, Psychology, Communications and IT.

It allows that budgetary limits imposed for economic crises can be better managed and accepted due to the reduction of costs of the judicial systems.

Artificial intelligence came to stay forever.

X. Bibliography References.

ClippingOnline, TRF3, *TRF3 100% PJe. PRESIDENTES DO CNJ E DO TRF3 LANÇAM PROJETO PARA REDUÇÃO E VIRTUALIZAÇÃO DO ACERVO DE PROCESSOS FÍSICOS DA JUSTIÇA FEDERAL DA 3.ª REGIÃO. Na primeira etapa, processos que tramitam em papel em 11 Subseções Judiciárias do Estado de São Paulo serão inseridos no PJe até o final de 2018.* http://web.trf3.jus.br/noticias/ClippingOnline/Noticia/Exibir/374929, published on Nov. 12, 2018, accessed on Dec. 15, 2018.

ClippingOnline. Thiago. Crepaldi. In Federal Judiciary Yearbook (Anuário da Justiça Federal 2019)*, launched on Nov. 21, 2018. Teto dos gastos públicos trava investimentos no TRF da 3ª Região*, http://web.trf3.jus.br/noticias/ClippingOnline/Noticia/Exibir/375348, published on Nov. 24, 2018, accessed on Dec. 15, 2018.

ClipplingOnline. Thiago Crepaldi and Damilo Vital. In *Justiça Federal será toda remanejada com o processo eletrônico*, http://web.trf3.jus.br/noticias/ClippingOnline/Noticia/Exibir/375142, published on Nov. 16, 2018, accessed on Dec. 17, 2018.

ClippingOnline, from the National Council of Justice – CNJ site. In *CNJ anuncia a criação de laboratório de inteligência artificial para o PJe*. http://web.trf3.jus.br/noticias/ClippingOnline/Noticia/Exibir/375711, published on Dec. 4, 2018, accessed on Dec. 17, 2018.

National Council of Justice – CNJ site, *Justiça em Números*, *in* http://www.cnj.jus.br/mwg-internal/de5fs23hu73ds/progress?id=02BblvxN38kXtXRYmmPZ6vmOT6QiI7qBOA_BxsQ-tFs, accessed on Dec. 15, 2018.

National Council of Justice – CNJ site, *Justiça Itinerante: juízes vão até os ribeirinhos da Amazônia*, *in* http://www.cnj.jus.br/noticias/cnj/85037-justica-itinerante-juizes-vao-ata-os-ribeirinhos-da-amazonia, accessed on Dec. 15, 2018

National Council of Justice – CNJ site, *Cadastro Nacional de Presos - BNMP 2.0*, http://www.cnj.jus.br/sistema-carcerario-e-execucao-penal/cadastro-nacional-de-presos-bnmp-2-0, accessed on Dec. 15, 2018.

JOTA site. Matheus Teixeira. *STF investe em inteligência artificial para dar celeridade a processos. Ferramenta Victor identifica se recursos se enquadram em repercussão geral e destaca, em segundos, peças principais*, https://www.jota.info/coberturas-especiais/inova-e-acao/stf-aposta-inteligencia-artificial-celeridade-processos-11122018?utm_source=JOTA+Full+List&utm_campaign=f280786d7c-EMAIL_CAMPAIGN_2017_10_06_COPY_01&utm_medium=email&utm_term=0_5e71fd639b-f280786d7c-380321969, published on Dec. 11, 2018, accessed on Dec. 17, 2018.

State Appeals Court of Sao Paulo site (Tribunal de Justiça), *Justiça itinerante*, *in* http://www.tjsp.jus.br/Especialidade/Itinerante, accessed on Aug 14, 2018.

Otonom Araçlar ve Ceza Hukuku

Doç. Dr. Eylem AKSOY RETORNAZ*

Giriş

Oya Baydar "Köpekli Çocuklar Gecesi" isimli ekolojik distopyasında *"(...) üç şeyin algoritması çıkarılamaz, üç şey var ki en gelişkin yapay zekaya bile aktarılamaz: hayal gücü, umut ve vicdan*"[1] demektedir.

Yazarın bu ifadelerinin mefhumu muhalifinden hayal gücü, umut ve vicdan dışındaki tüm alanlarda algoritmalarla yapay zekânın devreye girmesinin mümkün olduğu düşünülebilir. Nitekim kısmen ya da tamamen yapay zekâ barındıran bir sistem kontrolünde olan "otonom", "sürücüsüz", ya da "kendi kendini süren araçlar"[2], gündelik hayatımızda yer almaya başlamıştır.

Örneğin, İsviçre'nin Sion kentinde otonom bir araç, bir otobüs, 2016 yılından itibaren deneme amaçlı toplu taşıma hizmeti vermek üzere kullanılmaya başlanmıştır[3]. 2018 yılına kadar sorunsuz olarak hizmet vermeye devam eden bu araç bir otomobile çarpınca, kazanın nedenleri saptanıncaya kadar proje askıya alınmıştır[4].

Otonom araçlar söz konusu olduğunda ceza hukuku bakımından iki soru akla gelmektedir. Bu sorulardan ilki aracın sevk ve idaresinin doğrudan doğruya veya kısmen sürücü tarafından yapılmadığı hallerde ceza sorumluluğunun nasıl saptanacağıdır. İkinci soru ise gelişen teknolojiler aracılığıyla otonom araçlardan elde edilen verilerin iletilmesi kaydedilmesi veya kullanılmasının mümkün olup olmadığıdır.

Bu tebliğde bu sorulara yanıt aranmaya çalışılacaktır.

Ceza hukuku perspektifinden otonom araçları değerlendirmeye başlamadan önce, otonom araç kavramından ne anlaşılması gerektiği üzerinde durulmalıdır. Biraz önce de belirttiğimiz üzere

---

* Galatasaray Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı

[1] **Baydar** Oya, *Köpekli Çocuklar Gecesi*, Can Yayınları, İstanbul, 2019, s. 164.

[2] Bu tanımlamalar için bkz **Pekmez Kelep** Tuba, "Otonom Araçların Kullanımından Doğan Cezai Sorumluluk. Türk Hukuku Bakımından Genel Bir Değerlendirme", *Ceza Hukuku ve Kriminoloji Dergisi,* 2018; 6(2), s. 177. **Doğan** Koray, "Sürücüsüz Araçlar, Robotik Cerrahi, Endüstriyel Robotlar Ve Cezai Sorumluluk", D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN'a Armağan, C.21, Özel S., 2019, s. 3230.

[3] Project « "Smart Shuttle », https://www.postauto.ch/en/project-smartshuttle (Erişim Tarihi: 14/10/2019)

[4] https://www.rts.ch/info/regions/valais/9858744-la-circulation-des-navettes-autonomes-a-sion-suspendue-apres-un-accident.html (Erişim Tarihi: 14/10/2019)

otonom araçlar, kısmen ya da tamamen yapay zeka barındıran bir sistem kontrolünde olan araçlardır.

Söz konusu araçlar, herhangi bir sürücü müdahalesi olmadan, belirli bir rotada güvenli bir biçimde yol alabilen araçlardır[5]. Sürücüyü destekleyen güvenlik ve sürüş sistemleri otonom araç kavramının dışındadır.

Herhangi bir insan müdahalesi olmadan, başka bir ifadeyle bir sürücü olmadan yol alan bir araç bir yayaya çarpıp ölümüne sebep olduğunda, trafik güvenliğini tehlikeye düşürdüğünde veya biraz önce verdiğimiz örnekte olduğu gibi başka bir otomobile çarptığında ceza sorumluluğunun nasıl saptanacağı sorusu akla gelebilir.

Hemen ifade etmek gerekir ki suçun meydana gelmesi için suçun madde unsurlarının yanı sıra manevi unsurlarında da gerçekleşmiş olması gerekir[6]. Ayrıca bir kişinin davranışından dolayı cezalandırılabilmesi bu davranışın ona yüklenebilmesine diğer bir ifadeyle kusur yeteneğinin varlığına bağlıdır. Suçun maddi unsurlarından olan hareket insandan kaynaklanan harekettir. Bir hayvandan kaynaklanan hareket ancak insana atfedilebildiği ölçüde önem taşır.

Tüm bunlar ışığında tümüyle yapay zekâyla sevk ve idare edilen otonom araçların bir ceza sorumluluğunun olduğu söylenemez[7].

Otonom araçların seyri sırasında meydana gelen olaylarda kimlerin ceza sorumluluğunun söz konusu olabileceğini ardından da bu kişilerin hangi şartlarda sorumlu olacağını belirlemek gerekir. Bu kişiler sürücü veya aracı sevke ve idare eden kişi, programlayan kişi, üretici veya kullanıcı kişilerdir[8].

2918 sayılı Karayolları Trafik Kanununun 3. maddesinde yer alan tanıma göre sürücü, karayolunda motorlu ya da motorsuz taşıtları sevk ve idare eden kişidir. 1968 tarihli Birleşmiş Milletler Karayolları Trafik Sözleşmesi'nin[9] tanımlar başlıklı 1. maddesinin v. bendinde ise sürücü "bir motorlu taşıt *otomobil veya diğer taşıtları (bisiklet dahil) süren idare eden veya büyükbaş hayvanları yolda tek başına veya sürü halinde yönlendiren veya yolda yük veya binek hayvanlarını yönlendiren kişi*" olarak tanımlanmıştır.

Bununla birlikte TCK'nın tanımlara ilişkin 6. maddesinde ya da trafik güvenliğini tehlikeye sokma suçunun düzenlendiği 179. maddesinde ne sürücü ne de aracı sevk ve idare eden kişinin tanımı yapılmamıştır. Öğretide aracın sevk ve idaresinin doğrudan doğruya bizzat fail tarafından gerçekleştirilmesi gerektiği ifade edilmiştir.[10] Ancak failin mutlaka aracın içinde bulunmasının

---

[5] **Doğan**, s. 3230.
[6] **Zafer** Hamide, Ceza Hukuku Genel Hükümler TCK m.1-175, 7. Baskı, Beta Yayınevi, İstanbul, 2019, s. 276.
[7] Aynı yönde **Doğan**, s.3237-3238; **Kelep Pekmez**, s. 185.
[8] **Kelep Pekmez**, s. 186.
[9] Resmi Gazete Sayı: 28378 (Mükerrer) Tarih: 8/08/2012.
[10] **Soyer Güleç** Sesim, "Yeni Türk Ceza Kanunu'nda Trafik Güvenliğine Karşı İşlenen Suçlar", *Hukuki Perspektifler Dergisi*, 2006/9, s. 169; **Kılıçarslan İsfen** Sibel, *Alman Ve Türk Ceza Hukukunda Trafik Güvenliğini Kasten*

gerekmediği, aracın uzaktan kumanda edilmesinin mümkün olduğu da belirtilmiştir[11]. Bu doğrultuda, aracın seyri üzerinde hâkimiyet kuran kişinin aracı sevk ve idare eden kişi olarak nitelendirilmesi mümkündür.

Üretici ise aracın teknik donanımlarını çalıştıran tüzel kişidir. Programcılar ise aracın yazılım donanımını oluşturan kişilerdir. Aracın sevk ve iadresi sırasında meydana gelen suçlar abkımından üreticilerin taksirle ceza sorumluluğu gündeme gelebilir.

Kasten işlenen suçlar bakımından

Aracın sevk ve idaresine insan müdahalesinin söz konusu olduğu otonom araçların sürücüleri araç seyir halindeyken aracın sevk ve idaresinin sürücü tarafından devralınması yönündeki uyarıya rağmen sürücünün aracın sevk ve idaresini almaması sonucunda aracın başka bir araca çarparak diğer araçtaki kişinin ölmesi durumunda, aracın hızı, yolun durumu ve benzeri etmenler de dikkate alınarak sürücünün doğrudan kast veya olası kastla sorunmluluğu söz konusu olabilir.

Taksir sorumluluğu

Karayolları bakımından dikkat ve özen yükümlülüğünü Karayolları Trafik Kanunu ve ilgili yönetmelik ile belirlenen kurallar çerçevesinde belirlenmektedir. Aracın sevk ve idaresinin tamamen yapay zeka ile donatılmış bir sistemle gerçekleştirildği otonom araçlarda bakımından araçta yolculuk eden kişinin sisteme müdahale yükümlülüğünü de dikkat ve özen yükümlüğünün kaynağı olabilir[12]. Otonom araçta bulunan kişinin aracın sevk ve idaresini devralma yükümlülüğü bulunduğu takdirde gerekli dikkat ve özeni göstermediğinde taksir seviyesinde sorumluluğu söz konusu olacaktır[13].

Bununla birlikte, otonom araçta bulunan kişinin aracın sevk ve idaresini devralma yükümlülüğü bulumuyorsa usürücü koltuğunda otursa dahi test araçları hariç olmak üzere bu kişiden sürücüden beklenen dikkat ve özeni göstermesi beklenemez[14].

Tamanen otonom araçlar bakımından üreticinin belirli bir varsayımı öngörmediği ve bu nedenle eksik bir programlama yaptığı için bir kaza meydana geldiği takdirde üreticinin dikkat ve özen yükümlülüğünü ihlal ettiği bu nedenle taksir sorumluluğunun söz konusu olduğu düşünülebilir[15].

Tehlikeye Sokma Suçları, Seçkin Yayınevi, Ankara, 2013, s. 83; **Önok** Rıfat Murat, "Trafik Güvenliğini Tehlikeye Sokma Suçu", *TBB Dergisi* 2015 (121), s.162.162.

[11] **Koca** Mahmut, "Trafik Güvenliğini Kasten Tehlikeye Sokma Suçu (TCK 179/2, 3)", Kazancı Hakemli Hukuk Dergisi, Sayı 11, Temmuz 2005, s.102; **Önok**, s.162.

[12] **Kelep Pekmez**, s.189

[13] **Bénéjat**, s. 428.

[14] **Doğan**, ; **Bénéjat** Murielle, "Le droit pénal de la route face aux nouveaux modes de transport", *Actualité Juridique Pénal*, 2019, s. 428.

[15]**Heinrich** Bernd., (çev. Prof. Dr. Yener Ünver) "Otonom Araç Sürmekte Olası Cezalandırılabilirlik Riskleri", *Hukuk Köprüsü*, Cilt: 9, Sayı: 16, Haziran 2019, s.27.

Kişisel Verilerin Korunması

Otonom araçların geliştirilmesi diğer araçlarla veya servis sağlayıcılarla (bakım, onarım kişiselleştirilmiş sigorta, rehberlik vb. hususlarda iletişim kapasitelerinin de artması anlamına gelir. Veri alışverişi kapsamında, coğrafi konum sürüşle ilgili kontrol veya yardım, araç ve sürücüyle ilgili verilerin yoğun olarak aktarılması ve / veya giderek artan bir şekilde depolanması söz konusudur[16]. Bazı veriler sürücüleri yaşam tarzlarını (sık sık ziyaret edilen yerleri, programları, dinlenen müzikleri vb.) veya trafik kurallarının olası ihlallerini de ortaya koymaktadır.

Sonuç

Her türlü olasılığın düşünülerek programlamanın yapıldığı hallerde dahi karayolunda meydana gelen bazı olaylar nedeniyle kaza meydana gelebilir. Örneğin bir yayanın aniden yola fırlaması örneğinde olduğu gibi.

Otonom araçlar bakımından bir ikilem olarak ifade edilen bu durumda, araç fren mesafesinin kısalığı nedeniyle fren yapamayacak ya yayaya ya da direksiyonu kırdığı için bir ağaca çarparak araçta bulunan kişinin ölümüne yola açacaktır. Bu halde programı yapan kişi hangi yönde karar vermelidir? Bu örnekleri çoğaltmak mümkündür.

Bu sorulara hukuka uygunluk ve kusur ekseninde yanıt vermek mümkünken, otonom araç bakımından yanıt bulmak kolay değildir.

KAYNAKÇA

Altunç Mehmet Sinan Robotlar, "Yapay Zeka ve Ceza Hukuku", Pro*f. Dr. Feridun Yenisey'e Armağan*, İstanbul 2014.

Baydar Oya, *Köpekli Çocuklar Gecesi*, Can Yayınları, İstanbul, 2019.

Bénéjat Murielle, "Le droit pénal de la route face aux nouveaux modes de transport", Actualité Juridique Pénal, 2019.

Doğan Koray, "Sürücüsüz Araçlar, Robotik Cerrahi, Endüstriyel Robotlar Ve Cezai Sorumluluk", D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN'a Armağan, C.21, Özel S., 2019.

[16] **Jeanneret** Yvan, "Les aspects pénaux des véhicules automobiles sans conducteur", *Journées du droit de la circulation routière 23-24 juin 2016*, Stämpfli, 2016, s. 37-38

Heinrich Bernd., (çev. Prof. Dr. Yener Ünver) "Otonom Araç Sürmekte Olası Cezalandırılabilirlik Riskleri", Hukuk Köprüsü, C ilt: 9, Sayı: 16, Haziran 2019.

Jeanneret Yvan, "Les aspects pénaux des véhicules automobiles sans conducteur", *Journées du droit de la circulation routière 23-24 juin 2016*, Stämpfli, 2016.

Kılıçarslan İsfen Sibel, *Alman Ve Türk Ceza Hukukunda Trafik Güvenliğini Kasten Tehlikeye Sokma Suçları*, Seçkin Yayınevi, Ankara, 2013.

Koca Mahmut, "Trafik Güvenliğini Kasten Tehlikeye Sokma Suçu (TCK 179/2, 3)", Kazancı Hakemli Hukuk Dergisi, Sayı 11, Temmuz 2005

Küçüktaşdemir Özgür Yapay Zekânın Özgür İradesi ve Ceza Sorumluluğu Üzerine Bir Deneme.

Önok Rıfat Murat, "Trafik Güvenliğini Tehlikeye Sokma Suçu", *TBB Dergisi* 2015 (121)..

Pekmez Kelep Tuba, "Otonom Araçların Kullanımından Doğan Cezai Sorumluluk. Türk Hukuku Bakımından Genel Bir Değerlendirme", *Ceza Hukuku ve Kriminoloji Dergisi,* 2018; 6(2).

Soyer Güleç Sesim, "Yeni Türk Ceza Kanunu'nda Trafik Güvenliğine Karşı İşlenen Suçlar", *Hukuki Perspektifler Dergisi*, 2006/9.

Zafer Hamide, Ceza Hukuku Genel Hükümler TCK m.1-175, 7. Baskı , Beta Yayınevi, İstanbul, 2019.

Singularity Robotların ve Trans-Human Çağının Eşiğinde: Yapay Zekânın Ceza Sorumluluğu (On The Verge Of Singularity Robots and the Trans-Human Age: Criminal Responsibility of Artificial Intelligence)

Ezgi CANKURT[1]

GİRİŞ

Başlığı seçerken dahi, terimler konusunda defalarca düşündüren "Singularity" kavramı ve bu mantıkla tasarlanacak olan robotlara - özellikle düşünme ve hissedebilme yeteneklerinin aktarılabilmesi sonucunda – verilecek isimler henüz net değilken ; belirsizlik üzerine bazı ütopik yahut distopik olarak nitelendirilme tehlikesi barındıran öngörülerimizle, yapay zekanın ceza sorumluluğunu tartışmak istemekteyiz.

Başlıkta kullandığım üzere "singularity robot" tabiri yerine başka tabirler de gelebilir. Ancak ben özellikle yapay zekanın ilerleyebileceği noktaları henüz öngöremediğimiz için kavram kargaşası yaratmak istemeden, singularity kavramını açıklamak istemekteyim. İnsan zekasını aşacak, düşünebilen ve hissedebilen robotların var olacağı ve teknolojik tekillik kazanılacağı henüz teori aşamasındadır. Ancak halihazırda ele alınan kavramları açıklamak oldukça önemlidir.

Tebliğin tamamında anlatmaya çalıştıklarımız, günümüzden uzak ve distopik bir hikaye gibi değerlendirilebilir. Her dakika bilim insanlarının yapay zekanın mümkün oldukça ilerletilmesi için çalıştığını biliyoruz. Özellikle Avatar 2045 projesini gözardı etmemek gerekmektedir ve fakat teknolojik ilerleme noktasının sınırlarına dair belirsizlikler de var olmaya devam etmektedir. İnsan beyninn sanal ortama aktarılması ve hologramlaştırılması sonucunda, insanın ölümsüzleşmesini amaçlayan Avatar 2045 projesi hali hazırda devam etmektedir. Eğer Avatar 2045 projesi tamamlanırsa; insan bedeninde olan, yapay olarak insan beynine sahip ve hatta kişilik özellikleri olan insansı robotların hayatımızda olabileceği tahmin edilmektedir[2].

1. YAPAY ZEKA HAKKINDA GENEL BİLGİLER

1.1.KISA TARİHÇE

Özellikle düşünebilen makinaların varlığına dair, felsefi açıdan MÖ yıllarda ilk kez ele alındığını savunanlar da bulunmaktadır[3]. Robotlara ilişkin ilk izleri Japon Origami Sanatı ve daha da geriye "MÖ 150-100 yıllarına Ktesibios'un suyla çalışan otomatı"na götürenler olduğu gibi[4]; daha yakın tarihmizde Hobbes ve Descartes'in bilişsel zeka değerlendirmeleriyle de ele alınmaktadır[5].

Esasında bu konudaki ilk değerlendirme Alan Turing'e aittir. Turing; "Hesaplama Makineleri ve Zeka" adlı 1950 tarihli makalesinde; makinelerin düşünebileceğine dair değerlendirmeyi yapmıştır[6]. Yazmış olduğu bilimsel makalede özellikle sonuç bölümünde, *"Sonunda makinelerin tamamen entelektüel alanlardaki erkeklerle rekabet edeceğini umuyoruz. Ama başlamak için en iyileri hangileri? Bu bile zor bir karar. Birçok insan, satranç oynamak gibi çok soyut bir aktivitenin en iyisi olacağını düşünüyor. Makineye, paranın satın alabileceği en iyi duyu organlarını sağlamanın ve ardından İngilizce'yi anlamayı ve konuşmayı öğretmesinin en iyi yol olduğu da söylenebilir. Bu süreç bir çocuğun normal öğretimini takip edebilir. İşler belirtilebilir*

[1] Dr. Öğretim Üyesi- Beykent Üniversitesi Hukuk Fakültesi Ceza ve Ceza Usul Hukuku Anabilim Dalı
[2] Detaylar için bkz. http://2045.com/
[3] Nilsson, s.27 vd.
[4] Batukan, s.15.
[5] Ersoy, s.29.
[6] Say,s.83; Ford, s.262.

ve isimlendirilebilir, vb.Yine de doğru cevabın ne olduğunu bilmiyorum ama her iki yaklaşımın da denenmesi gerektiğini düşünüyorum." [7].

1.2.YAPAY ZEKA KAVRAMI VE ÇEŞİTLERİ

Yapay zekanın ceza sorumluluğu tartışmalarında; dar anlamda yapay zeka ve yapay genel zeka olarak ayrıma gidilmelidir. Özellikle çalışmamızda ele aldığımız, yapay genel zeka ve hatta ötesi açısındandır.

Yapay zeka, tanım olarak sürekli güncellenmektedir. Ancak *"zeki olsun yahut olmasın, bedensel etkinlikler dahil doğal sistemler tarafından yapılabilen bilişsel etkinlikler"* olarak kısaca tanımlayabiliriz[8]. Ancak *"karmaşık bir şeyi algılama ve uygun karar verme"* olarak da tanımlanabilmektedir[9].

Birçok sitede bize "beğenebileceğimiz" seçenekler sunulmaktadır. *"Benzer diğer kullanıcılar bunu beğendi, muhtemelen siz de beğenirsiniz."* önerilerini bize sunan yapay zekalara şaşırmıyoruz, ancak bizim neleri beğendiğimizi bizden daha iyi bilebilir mi sorusunu olumsuz yanıtlayabiliyoruz. Bu anlattığımız sadece, dar anlamda yapay zekanın yapabildiğidir. Bunu sadece *"şimdi izlemekte olduğunuzun ardından size önerecekleri yeni içerikleri aynı yollardan geçmiş milyonlarca diğer kullanıcıdan hangilerinin en uzun süre bağlandığına ve neyi ne sırada izlediğine göre eğitilen algoritmalarla belirler."*[10]

Otonom robotlar ise, *" bir kere aktive edilmesiyle beraber uzun süreler boyunca herhangi bir dış kontrol olmadan gerçek dünyada en azından belirli alanlarda faaliyet gösterebilen robot"* olarak tanımlanmaktadır[11].

Yapay öğrenme nedir diye ele alacak olursak, aslında *"bol miktarda girdi-çıktı dönüşümlerini makinenin kendisinin öğrenmesi"*dir. Sinir ağları prensibi ile bunun yapıldığını belirtmemiz gerekmektedir.Tekrar tekrar binlerce kez baştan başlayarak, her seferinde biraz daha gelişmiş bir öğrenme methodu gerekmektedir. Başlangıç açısından yapay öğrenmenin gerçekleşebilmesi için çok sayıda verinin hatta ve hatta milyarlarca verinin elinde bulunması ihtimali bulunmamaktayken; oyun bilgisayarlarındaki üç boyutlu hareketi canlandırmak için, bizzat oyun meraklıları için gelen talepler ve üzerine bizim birçok veriyi yüklediğimiz fotoğraflar sayesinde; derin öğrenme daha da ilerlemiştir[12].

Omuriliğindeki hasar sebebiyle on yılını felçli geçiren hastaya takılan protez, yapay genel zekanın işleyiş mantığını anlamamızı sağlayabilecektir. Takılan el protezinin üzerinde dokunma sensörü bulunmaktaydı ve sensörler de mikro elektrot kullanılarak insan beynine bağlanmıştı. Düşünce gücüyle elini hareket ettirebilmekte olan hastanın beynine aynı zamanda sensörlerden gelen sinyaller de iletiliyordu. Sanchez'in program yöneticisi olduğu bu gelişme sayesinde, hasta protez aracılığıyla artık gerçekten hissedebiliyordu [13].

---

[7] *"We may hope that machines will eventually compete with men in all purely intellectual fields. But which are the best ones to start with? Even this is a difficult decision. Many people think that a very abstract activity, like the playing of chess, would be best. It can also be maintained that it is best to provide the machine with the best sense organs that money can buy, and then teach it to understand and speak English. This process could follow the normal teaching of a child. Things would be pointed out and named, etc. Again I do not know what the right answer is, but I think both approaches should be tried. "* A. M. Turing (1950) Computing Machinery and Intelligence. Mind 49: 433-460, s.460. https://www.csee.umbc.edu/courses/471/papers/turing.pdf

[8] Say, s.83.

[9] Stanford Üniversitesi Yapay Zeka Laboratuvarı müdürü Sebastian Thurn tarafından yapılan tanımı nakleden Ersoy, s.29.

[10] Say, s.141.

[11] Ersoy, s.36.

[12] Say, s. 98-105.

[13] Eberl, s.320; ve basında "Dokunma hissi veren protez el yapıldı" olarak duyurulmuştu. Bkz. https://www.bbc.com/turkce/haberler/2015/09/150915_robot_el

Gelişmiş yapay zeka alanına, yani insanınkine benzer yapay zeka üzerindeki araştırmalara yapay genel zeka denilmektedir. Bu alanda çalışan 200 araştırmacıyla yapılan anket sonuçlarına göre; "%42'si düşünen bir makinenin 2030larda mümkün olacağına" inanmaktadır. Öte yandan sadece %2'si asla bu noktaya varılamayacağını düşündüğün belirtmiştir[14].

Özellikle syborg olarak adlandırılan robotlar, melez bir yapıdadır. *"Hem mekanik hem de etli bölümleri vardır."* Yapıları sebebiyle, hem biyolojik ve yapay zekaya sahip olabilirler[15].

Yapay zeka açısından ilk önemli nokta aslında, makinelerin dilbilim açısından insanları yakalamasıdır. Eğer gelişme sağlanırsa, artık kendi kendine e-mail yazabilecek ve konuşmalarını mantıklı çerçevede ilerletebilecektir. Böylelikle yapaz zekaların düşünebilmesi noktasında ortaya atılan Turing testi kriterini de geçebilecek noktaya varmış olurlar[16].

1.3.SINGULARITY/TEKNOLOJİK TEKİLLİK

Teknolojik tekillik, *"..insanlık tarafından tahmin edilemeyecek yeteneklere sahip süper akıllı makinelerin ortaya çıkması anlamına gelir."*[17] Tekillik/Singularity, kavramını teknolojik anlamda ilk kullanan kişi John von Neumann olarak kabul edilir.Neumann'ın 1950lerde ortaya attığı fikre göre; teknolojik anlamdaki ilerlemeler öyle bir noktaya ulaşacak ki, oradan sonrası insanlık adına tehlikeli olacaktır[18].

Tekillik açısından değerlendirmelerden IJ Good'un yaklaşımına göre; süper zekiler tarafından insanın zihinsel kapasitesinin üzerinde ve katlanarak artan daha zeki makinelerin tasarlanabileceği ve sonucunda da zeka patlaması yaşanacağı belirtilmektedir[19]. Bu noktadan sonra en zeki insandan dahi milyonlarca kat zeki olması demektir[20]. Alan Turing'in çalışma arkadaşı olan Good, bu yaklaşımıyla gelecekte olanın insan üzeri zekaya sahip olacağını ancak bu uysal makinelerdne kendilerini de nasıl denetim altına alabileceğimizi öğrenebileceğimizi de savunmaktaydı[21]. Hızla gelişen yapay zeka, gelişmeye devam edecek ve tekilliğe doğru devam edecektir[22].

Aslında tam olarak teknolojik tekillik tehlikesi, Vernor Venge'in "Yaklaşmakta Olan Teknolojik Tekillik" adlı makalesine dayanmaktadır. Venge, İnsanüstü zeka yaratılacağını ve insanlık çağının da bundan sonra sona ereceğini belirtmektedir[23]. Venge'e göre ;"*İnsan zekasını aşan bir zeka, ilerlemelere yön verdiğinde, bu ilerleme çok daha hılzı olacaktır. Aslında bizzat ilerlemenin, daha da kısa bir zaman ölçeğinde, daha zeki bir varlıklar yaratmayı içermemesi için hiçbir sebep yok."*[24]

Kurzweil ise, Vinge'den farklı düşünmektedir. Tekilliğin 2045 yılında yaşanacağını savunmakta olup; Kurzweil'e göre; beyine konulacak implantlar ile zekamız katlanacak ve makinelerle birleşme yaşayacağız[25]. Kurzweil, teknolojinin 2039'da ulaşabileceği noktanın günümüzle kıyaslanırsa; oldukça artacağını da savunmaktadır. Ayrıca bilinç sahibi ve duyguları olan robotların var olacağını iddia etmektedir[26]. Gelinecek olan düzeyde; ünlü yazar Asimov'un robot

---

[14] James Barrat, Our Final Invention:Artificial Intelligence and the End of the Human Era, New York: Thomas Dunne, 2013, s.196-197 'den aktaran Ford, s.263.
[15] Yazıcı,s.167.
[16] Tegmark, s.123-124.
[17] Potapov, 2018'den aktaran Yazıcı, s.165.
[18] Ford, s.265.
[19] Çelebi,2017'den aktaran Yazıcı, s.166, Ancak bunun için yapay zekaların daha ileri zekaya dönüşmesi gerekir. Bkz. Yazıcı, 166.
[20] Ford, s.264.
[21] Nilsson, s.663.
[22] Yazıcı, s.167.
[23] Vernor Venge, "The Coming Technological Singularity: How to Survive in the Post- Human Era", NASA VISION-21 Symposium, 30-31 Mart 1993 aktaran Ford, s.265 dip not 5 ve 6.
[24] Nilsson, s.664.
[25] Ford, s.266-267.
[26] Tegmark, s.204.

kurallarının[27] dışına çıkılacak ve dünyanın ilk vatandaşı olan Sophia gibi *„sadece insanlara tanınan hakları kullanmayı isteyen"*[28] sayıları milyarlara ulaşan robotlar olacaktır.

Kurzweil, teknolojik gelişmeleri çağlara ayırmaktadır. Bunların ilki fiziksel ve kimyasal düzeyde gerçekleşmiştir, devamında DNA ve ardından da sinir ağları ile devam etmiştir. Dördüncü çağ ise donanımsal ve yazılımsal olarak ilerlemeye devam etmektedir. Ancak insan zekası ile birleşilecek olan evre ve son olarak insan vücudunda yer alacak olan teknolojik gelişmeler[29].

Özellikle Kurzweil'in nanoteknoloji alanında da, biyolojimizin içersinde yer alacak olan nanobotlar ile sanal gerçeklik bize sinir sistemimiz ile yaşatılacağı iddiaları bulunmaktadır[30]. Nanoteknolojiye dair kısa bir değerlendirme yapacak olursak; Nanoteknoloji, teknolojik tekilliğin ileri bir boyututur. Minik bir fabrikanın istenilen herşeyi üretebilmesi olarak değerlendirmek gerekmektedir. Günümüz makinelerinin mikro ölçekli kopyalarıdır[31]. Aslında "moleküler boyutta makine" olarak adlandırılabilir[32].

Singularity'nin tam olarak bilim kurgu olduğunu ve insan zekasında robot üretebilmenin mümkün olsa bile çağlar ötesinde bir zaman diliminde ancak hayata geçirilebileceği de, Noah Chomsky tarafından savunulmaktadır. Hatta teknolojinin gelişme hızını gösteren Moore formülünü bulan Gordon Moore'a göre tekillik hala şüpheli durumdadır[33].

Öte yandan ise Musk ve Hawking, yapay zeka konusunda uyarılar yaptığını da hatırlatmalıyız. Hawking, Tegmark, Wilczek ve Russell gibi isimlerin özellikle yapay zekaya ilişkin uyarısına dikkat çekmekte ve özellikle düşünebilen bir bilgisayarın, *"para piyasalarından zengin olabilir, keşifleri araştırmacılardan daha hızlı yapabilir, insanları politikacılardan daha iyi manipüle edebilir, nasıl çalıştığını bile anlamadığımız silahlar geliştirebileceği"* şeklinde uyararaki konuya özellikle "bilim-kurgu" olarak yaklaşılmaması gerektiğinin altı çizmektedirler[34].

2. TÜRK HUKUKU AÇISINDAN DEĞERLENDİRME: KİŞİLİK KAVRAMI, HUKUKİ VE CEZA SORUMLULUĞU AÇISINDAN

Günlük hayatımıza dahil olan, yapay dar zeka ve ceza sorumluluğuna çalışmamızın kapsamının dışındadır. Yapay zekaların hepsi aynı özelliklere sahip değildir[35]. Bu nedenle hepsine aynı hukuki statünün tanınması da mümkün olamayacaktır. Herşeyden önce dar yapay zekalarda, üreten kişilerin ya da programcıların sorumluluğuna gidebilmemiz mümkündür.

TCK m.20/1 uyarınca*"Ceza sorumluluğu şahsidir. Kimse başkasının fiilinden dolayı sorumlu tutulamaz."* uyarınca, iradeleri olmayan yapay zekaya ilişkin olarak; elbette ki sorumluluk üreten, programlayan vb kişilerdedir[36]. Ancak kendi davranışları ile yeni bir illi fiil ile, somut olayın akışına dahil olabilecek nitelikteki yapay genel zekanın fiili sonucunda üreticinin yahut programlayıcının sorumluluğuna gidebilmek; objektif isnadiyet açısından mümkün görülmemektedir.

Robotların kişiliği var mıdır? Dünyada vatandaşlık verilen ilk robottan bahsetmiştik. Avrupa'da robotlara kimlik verilmesine ilişkin olarak tartışmalar çoktan başlamış durumdadır. Elektronik

[27] Bakınız detaylar için dip not 40.
[28] https://www.bbc.com/turkce/haberler-dunya-41780346
[29] Ersoy, s.169.
[30] Ersoy, s.171.
[31] Yazıcı, s.163.
[32] Ford, s.275.
[33] Ford, s.268-269.
[34] Ford, s.261 dip not 1.
[35] Aydemir, s. 26vd.
[36] Aydemir, s. 63.

kişilik verilmesi, Avrupa Parlamentosu açısından ele alınmaktadır[37]. Öte yandan yapay zekalara haklar verilmesinin önemini vurgulamak için, bazı varsayımları değerlendirmemiz gerekmektedir. Sürücüsüz/otonom araçlar bir kazaya sebep olursa, hukuki sorumluluğu kime aittir? Doktrinde bu konuda David Vladeck, arabanın kendisinin sorumlu olabilmesine imkan tanınması gerektiğini ve otonom araçların araç sigortası yaptırmaya mecbur tutulmasını önermektedir[38]. Ancak günümüz açısından yapay dar zeka olarak nitelendirebileceğimiz bu makineler; otonom ve yarı otonom olarak ayrılmaktadır[39]. Kaldı ki; böyle bir durumda sigorta yaptırmaya mecbur tutulan makinelere mülkiyet hakkı gibi hakların da tanınması zorunluluğu doğacaktır[40]. Ayrıca Türk Hukuku açısından otonom araçlara yönelik mevzuatın genelinde değişiklik yapılması gerektiği de önerilmektedir[41].

Türk Ceza Hukuku açısından hukuka aykırı bir fiilin varlığı cezalandırılması için yeterli değildir, fiilin mutlaka tipik olması da gerekmektedir[42]. Ceza sorumluluğunun şahsiliği ve sadece gerçek kişilerin fail olabileceği Türk hukuk sistemi açısından tercih edilmiştir[43]. Bunun sebebi de, *"belli bir gayeye yönelik irade ile hareket edebilme yeteneğinin sadece insanlara özgü"* olmasıdır[44]. Ancak tüzel kişilerin ceza sorumluluğuna dair teoriler varlığını sürdürmektedir. Ancak suç genel teorisi açısından fiilin de mutlaka insan davranışı olması gerekmektedir[45]. Bu nedenle, mevcut hukuk düzenimiz açısından; kendi iradeleri ve bilinçli olan robotlar üretilse dahi, bunlar tarafından işlenen fiiller açısından ceza sorumluluğuna gidilmesi mümkün değildir. Aksi bir uygulama kıyas yasağına açıkça aykırılık teşkil edecektir. Teknolojik tekilliğin iddia edildiği gibi gerçekleşmesi durumunda ise vereceğimiz cevaplar yetersiz kalabilir.

"Son İcadımız:Yapay Zeka ve İnsanlık Çağının Sonu" adlı kitabında yapay zekaya uygulanan *"meşgul çocuk senaryosu"* adı verilen bir idari tedbirden bahseden Barratt, araştırmacılardan oluşan bir grubun insan zekasına yaklaştığı sırada dış dünya ile bağlantısını kestiklerini ve kutuya hapsettiklerini belirtiyorlar. Bu noktada ise yapay zekanın araştırmacıları da kandırarak, onları manipüle etmeyeceğinin bir garantisi elbette olmayacaktır[46].

Roma Hukuku döneminde uygulanan kölelik kavramı benzeri bir statünün de uygulanabileceği de doktrinde tartışılmaktadır. Kölelik kavramının geri gelmesinin tehlikeleri bir yana, uygulama açısından da sıkıntılıdır. Eğer yapay zekanın sahibinin statüsü bir anlamda aile reisi olarak değerlendirilebilecek; bazı hak ve borçları sahibinin nezdinde de olsa üstlenebilecektir. Ancak burada uygulanma ihtimali olan, Noxa sorumluluğudur[47]. Bu durumda sahibi, zarar verilen şahsa

---

[37] Ersoy, s.89.
[38] Tegmark, s.146-147.
[39] *"otonom aracın sisteminin çalışmaya başladıktan sonra herhangi bir dış müdahaleye izin vermeksizin tamamen önceden yüklenmiş belirli bir program dâhilinde işlemesi durumunda tam otonom araçlardan7, ancak seyir halinde başka herhangi bir müdahaleye gereksinim duyan veya bunu mümkün kılan araçlar bakımından ise yarı-otonom araçlardan8 bahsetmek gerekmektedir."* Tanım ve detaylı bilgi için bkz. Tuba Kelep Pekmez, "Otonom Araçların Kullanımından Doğan Cezaî Sorumluluk: Türk Hukuku Bakımından Genel Bir Değerlendirme", Ceza Hukuku ve Kriminoloji Dergisi-Journal of Penal Law and Criminology 2018; 6(2):173-195, s.176.
[40] Tegmark, s.147.
[41] Kelep Pekmez, s.193.
[42] Koca/Üzülmez, s.109.
[43] Zafer, s.187.
[44] Koca/Üzülmez, s. 114.
[45] Zafer, s.186.
[46] James Barrat, Our Final Invention:Artificial Intelligence and the End of the Human Era, New York: Thomas Dunne, 2013, s.7-21 'den aktaran Ford, s.271.
[47] Bu görüşe göre, söz konusu dava Actio noxalis olacaktır. "*Haksız fiil işlemiş olan köle ya da aile evlâdının, efendisine veya aile babasına karşı, haksız fiilden zarar görmüş üçüncü kişilerin açabilecekleri davaya da actio noxalis denilmekteydi. Bu dava sonucunda, haksız fiili işlediği saptanmış olan köle ya da aile evlâdının ya zarar görmüş davacıya teslim edilmesi ya da davacının uğradığı zarar dolayısıyla saptanan para cezasının ödenmesi gerekmekteydi."* Actio noxalis tanımı için bkz. Gökçe Türkoğlu Özdemir, "Roma Hukukunda Actio de Peculio", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Cilt : 7, Sayı : 2, 2005, s.103-136, s.106.

robotu teslim edecek ve o da gerekirse imha edebilme yetkisine mi sahip olacaktır. Ya da ötesine götürülüp bırakılacak Tiber Nehri benzeri kurtarılmış alanlar mı oluşturulacaktır?

Esasında Teknolojik tekilliğe ne kadar yaklaşıldığına göre; verilecek cevaplar değişecektir. Otonom araçlar, insansız hava araçlar vb bakımından; programsal hatalardan kaynaklı durumlara ilişkin kast yahut taksirli suç tiplerinin de oluşturulması günümüzde de elzemdir. Ancak yapay dar zekalı robotlara; eğer sahipleri varsa günümüzdekilere benzer, hayvan idare edenlerin ceza sorumluluğunun yansımaları da görülebilir. Mutlaka tipik fiillerin varlığı açısından değerlendirme yapılacaktır.

Ceza hukukuna en çok ihtiyaç duyacağımız zaman aslında, yapay genel zekaların iyiliğe hizmet etmediği andır. Örneğin; *"Yapay zekanın, bizi suç işlerken gösterebilecek tamamen gerçekçi sahte videolar üretebilmeye başladığı anda"*[48] hukuki önlem için aslında geç kalınmış olunacağı açıktır.

Özellikle inceleme konumuz açısından yapay zekanın bilinçlendiği ve irade sahibi olduğu bir seviyeye ulaşılmış olsun yahut olmasın; yeni suç tipleri ihdas edilmeli ve/veya var olan suç tiplerine nitelikli haller arasına "robot kullanılarak" gerçekleştirilmesine dair yeni fıkralar eklenmelidir. Çünkü yapay zekanın kullanılarak bir suçun işlenmesi durumunda, suç işlemedeki kolaylık ve hızlı hareket edebilme ve hatta mağdurun teknolojik sistemler karşısındaki savunmasızlığı göz önünde bulundurulmalıdır.

Örneğin makinaya bağlı olan bir kimsenin tedavisinin, bilişim sistemin işleyişinin bozularak, yarıda kesilmesi durumunda; bu fiil günümüzde kasten öldürme sayılabilir mi? Dijital yollardan insan öldürme suçu olarak değerlendirebilir ve TCK 81, 82 veya garantör tarafından ise 83 uygulanabilir mi? Gereken dikkat ve özenin gösterilmemesiyle bu durum gerçekleşirse TCK m. 85 açısından tipik bir fiil söz konusu mudur? Serbest hareketli olarak işlenebileceğinden bir çoğumuz burada kasten yahut taksirle insan öldürme suçunun varlığını kabul edebilecektir? Hatta bilişim sistemine girme suçu da söz konusu olduğu için; belki de fikri içtima uygulanabileceği de savunulabilir. Yahut ameliyat esnasında yapay zeka kullanan bir cerrahın kullandığı sistemin çalışması kasten bozularak, hastanın sağlığının bozulması durumunda, ortada bilişim sistemine izinsiz giren kişi tarafından dijital yollarla işlenen bir kasten yaralama suçu mu mevcut mudur? Ceza hukukunda kıyas yasağı ve kanunilik ilkesi, yeni teknolojilerin varlığı sebebiyle yeni suç tiplerinin ihdas edilmesi gerekliliğinin ana gerekçeleridir.

3. ÖNERİLER

Yapay genel zekanın ortaya çıkmasından önce, insanlığın robotlara dair uluslararası etik değerler belirlemesi gerekmektedir[49]. Adı ister robot, ister makine yahut bilgisayar vb. nasıl adlandırılırsa adlandırılsın, artık düşünebilen ve bedenlere kavuşmuş yapay zekalara haklar ve yükümlülükler tanınmaması, en yalın tabirle kişilik verilmesi zorunlu olduğu teknolojik gelişmeler ile karşı karşıyayız[50]. Kaldı ki; *"Yapay zekanın yaratacağı tehditlere yönelik olarak tedbirleri hukuken ne kadar aldık?"* ve *"Yapay zekanın ceza sorumluluğunun olup olmadığı"* sorularının cevaplarını ancak robotlarının kişiliğinin olup olmadığına dair cevaplarımız şekillendirecektir. Burada da, teknolojik gelişmelere ne kadar hakim olduğumuzun yanıtını bizler kendimize vermek zorundayız. Aksi halde ceza sorumluluğunun tartışılması noktasında dahi, hukukçular olarak saf dışı bırakılabiliriz.

Bu bağlamda Fukuoka Dünya Robot Bildirgesi'ndeki ilkelerden bahsetmek gerekmektedir. İnsanların yol arkadaşları, destekçileri ve topluma katkı yapacak olan robotlara dair ilkeler[51],

[48] Tegmark, s.146.
[49] Tegmark, s.427.
[50] Eberl, s.341.
[51] Aydemir, s.32-33;Ersoy, s.40.

aklımıza yazar Asimov'un üç robot kuralını[52] getirmektedir. Öte yandan AB üyesi ülkelerde ise SPARC ve lex robotica oldukça önem kazanmaya başlamıştır[53]. Özellikle Horizon 2020'de robot etiği gibi konular ele alınmıştır[54]. Ayrıca euRobotics'in çalışmaları da oldukça önemsenmelidir[55].

Özellikle ölümcül robotlar yani silah kullanma yetkisi verilecek olan robotlar konusu birçok açıdan tehlike barındırmaktadır. Ancak otonomileri olan ve silahlanmış robotların Martens Kaydına aykırı olacağına dair görüş varlığını sürdürse bile, ölümcül robotların kullanılması durumunda; üstlerin her zaman robot eylemlerini öngörebilmelerinin mümkün olmaması ve günümüz ceza hukuku anlamında yaptırımın uygulanmasının da mümkün olmadığı gerekçeleriyle aşırı kaygı duyduğumu ve konunun bir an önce hukuki sınırlarının belirlenmesi gerektiği kanaatindeyim. Çünkü doktrinde de savunulduğu üzere, bu gibi durumlarda herhangi bir üretici, yazılımcı vb hatası bulunmamaktadır ve bu nedenle de robot fiilleri ile illiyet bağı kesilmektedir. İnsancıl hukuk açısından donanımı olmayan, ileri yapay zekada olmayan robotların daha tehlikeli olabileceği de doktrinde vurgulanmaktadır[56].

Teknolojik tekillik aşamasına ulaşılmış olsun yahut olmasın; karar mekanizması içerisinde hologram insanlar, trans insan olarak değerlendirilen yapay zeka, tekillik seviyesindeki süper zeka robotlar günümüzde de ve muhtemelen gelecekte de insan olarak kabul edilmeyeceklerdir. Anlattıklarımızı %1 doktrinine göre[57] hukukçular olarak değerlendirmemiz gerekmektedir. Asla gerçekleşmeyeceği anlayışının insanlığa yararı yoktur. Ancak mevcut gelişmeler ışığında öngörülmektedir ki ; kişilik kazanacak olan yapay zekanın ceza sorumluluğuna ilişkin ilkeler mili ceza kanunlarında da yer almaya başlayacaktır. Bu noktada bizim de hukuk sistemimize dahil etmemiz uygun olacaktır.

Yapay zeka açısından aydınlatma da oldukça önemlidir. Bireylerin ilişkili oldukları yapay zeka hakkında, üreticiler tarafından var olan veya olası olumlu ve olumsuz etkilerinin paylaşılması gerekmektedir. Bir ilacın yan etkisinin paylaşılması beklenirken, kullanılan yapay zeka açısından da aydınlatılmak önemlidir. Ve hatta bu konuda dolandırılmadığımızı bilmek de önemlidir. Şimdilik yapay zekanın eşya olduğu kabul edildiği için, en azından bu açıdan neye sahip olduğumuzu bilmemiz gerekmektedir. Çünkü kişisel verilerimizle oldukça yakın ilişkili yapay zeka bizimle birlikte gelişmekte ve ilerlemekte ve hatta güncellenmektedir. En azından sahip olduğumuz ürünlerin hangi aşamaya kadar güncellenebildiğini bilmemiz gerekmektedir. Bireylerin evrensel değerleri açısından da bu önemlidir. Aydınlatmanın ihlaline ilişkin olarak özle ve kamu hukukunun karakterlerine uygun ölçüde düzenlemeler yapılmalıdır.

Bu konuda özellikle birkaç olasılığı da ileri sürmem gerekmektedir. Robot kopyaların ders verdiği ve dersin ancak bitiminde, kürsüdeki varlığın robot olduğunun anlaşıldığı olaylar dünyada yaşanmaktadır. Özellikle otonom silah endüstrisi ve katil robotlar kavramı da, bilim insanları açısından endişe vermeye başlamıştır. Eğer Kurzweil'ın tahmini gerçekleşirse, tasarlanan insan-makine karışımı "Trans Human Çağı" makinenin hızı ve zekâsı insan zihnine entegre edilecektir. Bilim insanları, bu teknolojinin insanlığa birkaç seviye atlatacağını ve daha keskin bir beyin yapısının ortaya çıkacağını düşünülmektedir. Konuyu bu kadar tehlikeli kılan ana unsur da budur .

Musk, süper zekaların insanlığı yoketmesini engellemek için, insanlığın ve makinelerin birbirleriyle telepatik iletişim kurabileceklerine dair öngörülerde bulunmaktadır[58].

---

[52] *"Asimov Yasaları: 1- Bir robot, bir insana zarar veremez ya da zarar görmesine seyirci kalamaz. 2- Bir robot, birinci kuralla çelişmediği sürece bir insanın emirlerine uymak zorundadır. 3- Bir robot, birinci ve ikinci kuralla çelişmediği sürece kendi varlığını korumakla mükelleftir."* Aktaran Batukan,s.35; ayrıca bkz. Nilsson, s.25-26.

[53] AB üyelik sürecinde ülke olarak Türkiye'nin de AB'deki gelişmeleri dikkatle izlemesi gerektiği hakkında bkz. Aydemir, s. 34.

[54] AR-GE ve Avrupa Dijital İnovasyon Ağı hakkındaki açıklamalar için bkz. Aydemir, s.36-37.

[55] Ersoy, s.46.

[56] Ersoy, s.99-109,111.

[57] *"Gerçekleşme ihtimali çok düşük olsa bile, gerçekleşirse sonuçları çok korkunç olacağı için yine de ciddiye almamız gerekir."* Bkz. Ford, s.272.

[58] Yazıcı, s.165.

Klonlama yasağına benzer şekilde, insansı yahut trans insan robotların üretilmesi ve kullanılması da tamamen yasaklanabilir yahut özel izinler verilerek kullanılabilir. Yapay zekanın gelişmesi özellikle insan onuru kavramı açısından yeniden düşünmeye itmektedir. Ancak ceza hukuku sorumluluğu alanında çalışmamızı sınırlandırdığımız için, Yapay zeka onuru üzerinde de düşünülmesi gerektiğini de vurgulamak isterim.

SONUÇ YERİNE

Yapay genel zekanın ortaya çıkmasından önce, insanlığın robotlara dair uluslararası etik değerler belirlenmelidir. Düşünebilen ve bedenlere kavuşmuş yapay zekalara haklar ve yükümlülükler tanınması ve kişilik verilmesi ilk olası hukuki gelişmelerdir. Özellikle de robot onuru kavramı ve insanların robotlardan korunmasına dair düzenlemeler de; robotların insanlardan korunması kadar önemsenmelidir.

Robot kavramının, Slav dillerindeki anlamı *"birisinin kölesi olmak"*tır[59]. İnsanlar robotları köleleştirmek için üretmiştir, şu an ise ayrılamaz bir bağımlılık yaşar hale gelmiştir. Ütopya ve distopya arasına sıkışan insanın, süper zekalara ve trans insana vereceği ilk tepkiler ne olacaktır?[60] Denetlemek, yasaklamak, geliştirmek, yardım etmek, uyum sağlamak, anlamaya çalışmak…? Tartışılır.

Öte yandan ceza kanunlarında fail olarak nitelendirilseler dahi, günümüz anlamında yaptırımların yapay zekalar açısından uygulanabilirliği tartışmalıdır. Ceza sorumluluğu, fail, mağdur ve hatta daha doğru bir anlatımla; başta suç tipleri olmak üzere, suç genel teorisi ve yaptırım teorisinin teknolojik gelişmelere göre gözden geçirilmesi gerekmektedir. Günümüz haliyle ceza hukuku; yapay genel zeka olarak adlandırdığımız robotların, süper zekaların ve trans insan açısından yetersiz kalacaktır. Bunun için ceza hukuku üzerine yeniden düşünmek ve hatta karşıtından yola çıkmak da gerekebilir. Uluslararası koruma sistemlerinin ve evrensel etik ilkelerin belirlenmesinin aciliyet taşıdığı yapay genel zeka açısından, insanlığın aydınlatılması da gerekmektedir. Teknolojik gelişmelerin seviyesini bilemeden, Robot Hukuku açısından değerlendirmeler yapılması dayanaksız ve eksik kalacaktır. Özellikle kişilik açısından gelişmelerin beraberinde, suç teşkil eden fiilin insandan kaynaklanması gerekliliğine dair yerleşik tanımlar açısından da yapısöküm gerçekleşecektir.

Kaynaklar

A. M. Turing (1950) Computing Machinery and Intelligence. Mind 49: 433-460. https://www.csee.umbc.edu/courses/471/papers/turing.pdf

Ayşe Meriç Yazıcı, "Yapay Zeka ve Nanoteknoloji", Yapay Zeka ve Gelecek, Ed. Gonca Telli, Doğu, 2019.

Can Batukan, Robo-Tizm, Altıkırkbeş, 2017.

Cem Say, 50 Soruda Yapay Zeka, Bilim ve Gelecek Kitaplığı-59, 13.Baskı, Yedi Renk,2019.

Çağlar Ersoy, Robotlar, Yapay Zeka ve Hukuk, 4. Baskı, On İki Levha, 2019.

Gökçe Türkoğlu Özdemir, "Roma Hukukunda Actio de Peculio", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Cilt : 7, Sayı : 2, 2005, s.103-136.

Hamide Zafer, Ceza Hukuku Genel Hükümler (TCK m.1-75), 7.Baskı, Beta, 2019.

[59] Batukan, s.16.

[60] *"Ya da yapay zekanın gelecekte gelişmesiyle şekillenen farklı teknoloji demetleri insanı neye dönüştürecektir?"* bkz. Yazıcı, s.169.

Mahmut Koca/İlhan Üzülmez, Türk Ceza Hukuku Genel Hükümler,11. Baskı, Seçkin, 2018.

Martin Ford, Robotların Yükselişi, 3. Baskı, Kronik, 2018.

Max Tegmark, Yaşam 3.0, Pegasus, 2019.

Melisa Aydemir, "Yapay Zekalı Robotların Ceza Sorumluluklarının Araştırılması", Suç ve Ceza Dergisi, 2018 SAYI: 4.

Nils J. Nilsson, Yapay Zeka Geçmişi ve Geleceği, 2. Baskı, Çev. Mehmet Doğan, Boğaziçi Üniversitesi, 2010.

Ulrich Eberl, Akıllı Makineler, Paloma, 2019.

http://2045.com/

https://www.bbc.com/turkce/haberler/2015/09/150915_robot_el

https://www.bbc.com/turkce/haberler-dunya-41780346

İnternette İşlenen Hakaret Suçları

Araş.Gör. Dr. Tuba KELEP PEKMEZ

Konumuz olan internette işlenen hakaret suçlarının kanunlarımızda özel bir düzenlemesi mevcut bulunmamaktadır. Dolayısıyla TCK m. 125 ve devamında yer alan hakaret suçuna ilişkin düzenlemeler esas alınmakta; delil elde edilmesi ispat ve tespiti bakımından ise internet kanunu ile Yargıtay kararları göz önünde bulundurulmaktadır.

Hakaret suçlarının internet ortamında gerçekleştirilmesinde özellik arz eden hususları belirlemeden önce hakaret suçu ile ilgili olarak genel bir değerlendirme ve bilgilendirme yapılmalıdır. Daha sonra hakaret suçlarının internette gerçekleştirilmesine ilişkin tartışmalar ve çözümlere yer verilecektir.

Hakaret Suçu tipiyle ilgili genel bilgiler

Hakaret suçu TCK m. 125'te düzenlenmektedir. Buna göre (*1) Bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat eden (...) (1) veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldıran kişi, üç aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Mağdurun gıyabında hakaretin cezalandırılabilmesi için fiilin en az üç kişiyle ihtilat ederek işlenmesi gerekir. (2) Fiilin, mağduru muhatap alan sesli, yazılı veya görüntülü bir iletiyle işlenmesi halinde, yukarıdaki fıkrada belirtilen cezaya hükmolunur. (3) Hakaret suçunun; a) Kamu görevlisine karşı görevinden dolayı, b) Dini, siyasi, sosyal, felsefi inanç, düşünce ve kanaatlerini açıklamasından, değiştirmesinden, yaymaya çalışmasından, mensup olduğu dinin emir ve yasaklarına uygun davranmasından dolayı, c) Kişinin mensup bulunduğu dine göre kutsal sayılan değerlerden bahisle, İşlenmesi halinde, cezanın alt sınırı bir yıldan az olamaz. (4) (Değişik: 29/6/2005 – 5377/15 md.) Hakaretin alenen işlenmesi halinde ceza altıda biri oranında artırılır. (5) (Değişik: 29/6/2005 – 5377/15 md.) Kurul hâlinde çalışan kamu görevlilerine görevlerinden dolayı hakaret edilmesi hâlinde suç, kurulu oluşturan üyelere karşı işlenmiş sayılır. Ancak, bu durumda zincirleme suça ilişkin madde hükümleri uygulanır"*

Belirtmek gerekmektedir ki hakaret suçunun cezalandırılabilirliğine ilişkin koşullar m. 125'te yer alan düzenleme ile sınırlı değildir[1]. Nitekim m. 126, 127, 128 ve 129'ta suçun maddi unsurları, hukuka aykırılık unsuru ve kusurluluk ile ilişkili düzenlemeler yer almaktadır.

Korunan Hukuki Değer

Hakaret ve sövme suçlarında korunan hukuki yarar, sosyal bir kavram olarak şereftir[2]. Hakaret suçlarında korunan hukuki değer kişinin hem sübjektif hem de objektif şerefidir[3]. Bu durumda bu suçla korunan hukuki değer karma bir hukuki değer olup hem kişinin kendisine karşı sahip olduğu içsel bir değer olarak şerefi hem de kişiler nezdindeki değerini ifade etmektedir. Bu durumda TCK m. 125'te bahsedilen kişinin onur ve şerefi iç şerefi ifade ederken, dış şeref ifadesi ise saygınlık olarak yer bulmuştur.

Fail: Hakaret suçları bakımından failin bir özellik arz etmesi gerekmemektedir. Dolayısıyla herkes bu suçun faili olabilmektedir. Belirtmek gerekir ki tüzel kişiler bakımından hakaretin tüzel kişinin organı veya temsilcisi tarafından gerçekleştirildiği durumlarda tüzelkişiler bakımından bir güvenlik tedbiri uygulanması mümkün değildir, dolayısıyla bu gibi durumlarda tüzel kişi nezdindeki organda görev alan ve temsil yetkisine sahip kişilerin cezalandırılması söz konusu olacaktır[4].

---

[1] Mahmut Koca/İlhan Üzülmez, Türk Ceza Hukuku Özel Hükümler,Adalet, 2018, s. 469.

[2] ÖZGENÇ, İzzet, Türk Ceza Kanunu Gazi Şerhi (Genel Hükümler), Ankara:Seçkin Yayıncılık, 2005, s. 854; SAVAŞ, Vural/MOLLAMAHMUTOĞLU, Sadık, Türk Ceza Kanununun Yorumu C:4, Ankara:Seçkin Yayınevi, 1995,s.4756); Koca/Üzülmez, s. 469.

[3] Nitekim madde gerekçesinde korunan hukuki değerle ilgili olarak "Hakaret fiillerinin cezalandırılmasıyla korunan hukuki değer kişilerin şeref, haysiyet ve namusu, toplum içindeki itibarı, diğer fertler nezdindeki saygınlığıdır" ifadelerine yer verilmiştir.

[4] Ahmet Caner Yenidünya/Mehmet Ali Alşahin, Bireyin Şerefine Karşı Suçlar, TBB Dergisi, 2007/68, s. 45;

Hakaret suçlarının basın yoluyla işlenmesi durumunda ise fail 5187 sayılı Basın Kanunu m. 11'e göre belirlenecektir[5].

Hakaret suçunun internet ortamında işlenmiş olması halinde, hakaret içeren sözlerini kullanan, yazan kişi suçun failidir. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun 4.maddesi uyarınca içerik sağlayıcılar da hakaret suçunun faili olabilirler.

Söz konusu bu düzenlemeden de anlaşılacağı üzere, içerik sağlayıcılar internet ortamında kullanıma sundukları her tür içerikten sorumludurlar, içerik sağlayıcı bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak sunuş biçiminden, sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça anlaşılmakta ise genel hükümlere göre sorumludur.

Mağdur: Suç mağdur bakımından da bir özellik göstermemektedir[6]. Nitekim bu husus maddede yer alan "bir kimseye" ve "bir kimsenin" ifadeleri ile işaret edilmektedir[7]. Bu bağlamda suçla korunan hukuki değer olan şeref, kişilerin buna ilişkin içgörülerinden ve kendilerine yönelik farkındalıklarından bağımsız bir şekilde korunmaktadır. Dolayısıyla çocuklar veya akıl hastaları gibi kişilerin de bu suçun mağduru olabilmesi mümkün kabul edilmekte, hatta bir kimsenin toplum nazarında şereften yoksun olarak bilinmesi durumunda dahi korunması gereken bir saygınlıklarının olduğu kabul edilerek bu suçun mağduru olabilecekleri belirtilmektedir[8].

Doktrinin bir kısmına ve Yargıtay'a göre tüzelkişiler bu suçun mağduru olamazlar[9]. Gerçekten de şerefin yalnızca gerçek kişilerin sahip olabileceği manevi bir varlık olmasından dolayı tüzel kişilerin bu suç bakımından mağdur olmaları mümkün olmaz. Ancak tüzel kişiler bu suç bakımından suçtan zarar gören olabilirler. Bununla bağlantılı olarak *kişi topluluklarının* söz konusu suçun mağduru olup olamayacağı ayrıca tartışılmaktadır. Burada kişi topluluğunun açıkça sınırlandırılmış ve belirlenmiş olması, belirli ve teşhis edilebilir kişilerle ilişkilendirilmesi topluluğun suçun mağduru olması için aranan koşul olarak görülse de[10], kanaatimizce burada toplulukta bulunan her bir kişiye karşı tek bir fiille gerçekleştirilen birden fazla hakaret suçu

---

[5] **Söz konusu hüküm şu şekildedir: "***Basılmış eserler yoluyla işlenen suç yayım anında oluşur.*
Süreli yayınlar ve süresiz yayınlar yoluyla işlenen suçlardan eser sahibi sorumludur.
Süreli yayınlarda eser sahibinin belli olmaması veya yayım sırasında ceza ehliyetine sahip bulunmaması ya da yurt dışında bulunması nedeniyle Türkiye'de yargılanamaması veya verilecek cezanın eser sahibinin diğer bir suçtan dolayı kesin hükümle mahkûm olduğu cezaya etki etmemesi hallerinde, sorumlu müdür ve yayın yönetmeni, genel yayın yönetmeni, editör, basın danışmanı gibi sorumlu müdürün bağlı olduğu yetkili sorumlu olur. Ancak bu eserin sorumlu müdürün ve sorumlu müdürün bağlı olduğu yetkilinin karşı çıkmasına rağmen yayımlanması halinde, bundan doğan sorumluluk yayımlatana aittir.
Süresiz yayınlarda eser sahibinin belli olmaması veya yayım sırasında ceza ehliyetine sahip bulunmaması ya da yurt dışında olması nedeniyle Türkiye'de yargılanamaması veya verilecek cezanın eser sahibinin diğer bir suçtan dolayı kesin hükümle mahkûm olduğu cezaya etki etmemesi hallerinde yayımcı; yayımcının belli olmaması veya basım sırasında ceza ehliyetine sahip bulunmaması ya da yurt dışında olması nedeniyle Türkiye'de yargılanamaması hallerinde ise basımcı sorumlu olur.
Yukarıdaki hükümler, süreli yayınlar ve süresiz yayınlar için bu Kanunda aranan şartlara uyulmaksızın yapılan yayınlar hakkında da uygulanır." Belirtmek gerekir ki Basın Kanununda yer alan bu hüküm ceza sorumluluğunun şahsiliği ilkesine aykırı olması nedeniyle eleştirilmektedir. Bkz.: Ahmet Caner Yenidünya/Mehmet Ali Alşahin, Bireyin Şerefine Karşı Suçlar, TBB Dergisi, 2007/68, s. 46; Tezcan, Erdem, Önok, Teorik ve Pratik Ceza Özel Hukuku, ONALTINCI Baski, Seçkin, Ankara, Eylül 2018; Koca/Üzülmez, s. 471.

[6] Belirtilmelidir ki hakaret mağdurunun yaşayan bir kimse olması gerekmektedir. Zira ölen kişiler bakımından gerçekleştirilen aşağılama veya sövme fiilleri ölenin hatırasına hakaret suçu olarak TCK m. 130'da ayrı bir suç olarak cezalandırılmaktadır.

[7] Koca/Üzülmez, s. 471

[8] Ahmet Caner Yenidünya/Mehmet Ali Alşahin, Bireyin Şerefine Karşı Suçlar, TBB Dergisi, 2007/68, s. 48; Tezcan, Erdem, Önok, Teorik ve Pratik Ceza Özel Hukuku, ONALTINCI Baski, Seçkin, Ankara, Eylül 2018; Koca/Üzülmez, s. 471.

[9] *"TCK'nın 125. Maddesine göre hakaret suçunda şeref ve saygınlığı rencide edilebilecek nitelikte sözlerin gerçek kişilere yöneltildiğinde hakaret suçunu oluşturabileceği, herhangi bir gerçek kişi ile arasında aidiyet ilişkisi kurulmadan tüzel kişiye söylenen sözlerin bu kapsamda değerlendirilemeyeceği"* (Y18CD, 6.2.2017, 18978/1193); Koca/Üzülmez, s. 471; Ahmet Caner Yenidünya/Mehmet Ali Alşahin, Bireyin Şerefine Karşı Suçlar, TBB Dergisi, 2007/68, s. 48; Karşıt görüş için bkz: Özbek, Şerefe Karşı Suçlar, s.258; Tezcan/Erdem/Önok, s. 455; Önder, Şahıslara Karşı, s. 228; Erman/Özek, Kişilere, s. 260.

[10] Tezcan, Erdem, Önok, Teorik ve Pratik Ceza Özel Hukuku, ONALTINCI Baskı, Seçkin, Ankara, Eylül 2018, s. 591; Centel/Zafer, Çakmut, Kişilere Karşı Suçlar, s. 224)

oluşacağını ve dolayısıyla aynı neviden fikri içtima hükümlerinin bu gibi durumlarda uygulanması gerektiğini söylemek isabetli olacaktır[11]. Ancak burada dikkat edilmesi gereken husus topluluğa yöneltilen ve hakaret içeren fiillerin belirli ve sınırlanmış kişilerle ilişkilendirilmesi gerekliliğidir. Eğer topluluğa yönelik bir hakarette kişiler sınırlanıp belirlenemiyorsa bu durumda suçun oluşmadığını kabul etmek gerekir[12]

Hakaret suçunda mağdurun belli veya belirlenebilir olması gerekmektedir. Dolayısıyla hakaret içeren ifadede mağdurun isminin açıkça zikredilmesi bir zorunluluk arz etmez. Mağdurun kim olduğunun kullanılan ifadeden anlaşılabilmesi suçun oluşması için yeterli kabul edilmektedir[13]. Nitekim TCK m. 126'da bu husus *"hakaret suçunun işlenmesinde mağdurun ismi açıkça belirtilmemiş veya isnat üstü kapalı geçiştirilmiş olsa bile, eğer niteliğinde ve mağdurun şahsına yönelik bulunduğunda duraksamayacak bir durum varsa, hem ismi belirtilmiş ve hem de hakaret açıklanmış sayılır"* şeklinde belirtilmiştir. Bu hususa "matufiyet" şartı adı verilmektedir. Yargıtay bu şartın uygulanmasında esnek davranmaktadır. Dolayısıyla matufiyetin gerçekleşmesi için objektif olarak mağdurun belirtildiğinin anlaşılıyor olması yeterli görülmektedir[14].

Suçun Konusu: Korunan hukuki değer ve konu bu suçta birleşmiştir. Bu anlamda suçun konusunu da onur, şeref ve saygınlık olarak ifade edilmesi gerekmektedir. Bu noktada ise vurgulamak gerekmektedir ki bu suç bir tehlike suçudur. Bu anlamda suçun konusunun bir zarara uğramış olması bu suç bakımından aranmaz. Hatta suçun konusuna ilişkin tehlikenin somut olarak ortaya çıkması da gerekmez. Dolayısıyla isnadın veya değer yargısının kişinin onur, şeref ve saygınlığını rencide edebilecek nitelikte olması yeterlidir. Bu anlamda suç bir soyut tehlike suçudur[15].

Fiil: Serbest hareketli suç olup, sözler, imalı şarkılar, yazı, çizim, resim, nefreti gösteren hareketler ve bunun gibi davranışlarla işlenebilir. Aynı şekilde, telefonla, mektupla, basın yayın

---

[11] Koca/Üzülmez, s. 473;

[12] Koca/Üzülmez, s. 473; Yenidünya/Alşahin, s. 48; Bununla birlikte 125/5 uyarınca kurul halinde çalışan kamu görevlilerine görevlerinden dolayı hakaret edilmesi halinde suç kurulu oluşturan üyelere karşı işlenmiş sayılacak, ancak bu durumda zincirleme suça ilişkin madde hükümleri uygulanacaktır.

[13] Tezcan, Erdem, Önok, Teorik ve Pratik Ceza Özel Hukuku, ONALTINCI Baski, Seçkin, Ankara, Eylül 2018; Dönmezer, Kişilere Karşı Suçlar, no: 216; Erem/Toroslu, Ceza Hukuku Özel Hükümler, s. 437; Centel/Zafer, Çakmut, Kişiere Karşı Suçlar, s. 224; Özbek, İzmir Şerhi, s. 860)

[14]. Tezcan, Erdem, Önok, Teorik ve Pratik Ceza Özel Hukuku, ONALTINCI Baskı, Seçkin, Ankara, Eylül 2018, s. 588; Aynı yönde bkz: Ayhan Önder, Şahıslara Karşı Cürümler, s. 222); *"Katılanın müdür olarak görev yaptığı okulun kantin görevlisi olan sanığın, aynı okulun öğrencisi olan tanığın facebook hesabında paylaştığı "sizin okul müdürü de gözlüklü veya kel mi" şeklindeki gönderinin altına "bizim müdür o... ç..." şeklinde hakaret içerikli sözler yazması biçimindeki eyleminde, sanığın bu sözleri kime hitaben yazdığı hususundaki çelişkili beyanları ile tüm dosya kapsamı birlikte değerlendirildiğinde, bu sözlerin katılanın şahsına yönelik bulunduğunun anlaşılması karşısında, sanığın atılı suçtan mahkumiyeti yerine "TCK'nın 126. maddesinde belirtildiği şekilde mağdurun isminin açıkça belirtilmemiş olması ve söylenen sözün mağdurun şahsına yönelik bulunduğuna dair duraksanmayacak bir açıklık bulunmadığı" şeklindeki yerinde olmayan gerekçeyle beraat kararı verilmesi,"*(Y18CD, E. 2015/4274 K. 2015/3760 T. 1.7.2015, (Kazancı İçtihat Bankası); *"Sanığın hayvanlarını beslediği M... Köyü muhtarı olan katılan O.'a köy camisinin önünde "... Benim hayvanlarımdan kim rahatsız oldu, boynuzları bir yerine mi battı, beni kim şikayet ettiyse hayvanların boynuzu k...çına girsin, kim şikayet ettiyse lafım ona..." biçimindeki sözler ile hakaret ettiği, bu sözlerin tanıklar tarafından duyulduğu ve her ne kadar sanık hakaret içerikli sözlerinde katılanın ismini zikretmemiş ise de bunun katılana yönelik olduğunun herkes tarafından bilindiğinin tanık beyanları ile doğrulanması karşısında, TCK'nın 126/1. maddesinde düzenlenen; "Hakaret suçunun işlenmesinde mağdurun ismi açıkça belirtilmemiş veya isnat üstü kapalı geçiştirilmiş olsa bile, eğer niteliğine ve mağdurun şahsına yönelik bulunduğunda duraksanmayacak bir durum varsa hem isim belirtilmiş hem de hakaret açıklanmış sayılır." hükmü karşısında, sanığın katılana hakaret ettiğinin kabulü ile hükümlülük kararı verilmesi gerekirken, hakaret içeren sözlerinin katılana yönelik olmadığı şeklindeki yerinde olmayan gerekçeyle beraat kararı verilmesi*" (YARGITAY 18. CEZA DAİRESİ E. 2015/3116 K. 2015/3572 T. 29.6.2015); *"Matufiyet yargısal kararlarda, yayın ile şeref ve haysiyetine veya özel yaşamına dolayısıyla kişilik haklarına saldırıda bulunulduğunu iddia eden yönünden varlığı aranan önemli bir koşul olarak tarif edilmiş, matufiyetin varlığını kabul için o yayında veya konuşmada, ya kişinin adından açıkça söz edilmesi ya da konumunun, sıfatının gösterilmesi veya bunlardan söz edilmese dahi yayın içeriğinden bu kişinin amaçlandığı, sözlerin ona yönelik olduğunun anlaşılması veya anlaşılabilir olması şartları aranmıştır.Hukuka aykırı eylemde bulunan kişi mağdurun ismini açıkça belirtmemiş veya isnat ettiği fiili üstü kapalı bir biçimde geçiştirmişse, isnadın mahiyetinde ve mağdurun şahsına matufiyetinde tereddüt edilmeyecek derecede karineler varsa, hem isim zikredilmiş, hem de hakaret vaki olmuş sayılır* (Hukuk Genel Kurulu 16/09/2015 gün ve 2014/4-85 E 2015/1774 K-07/07/2010 gün ve 2010/4-377 E 2010/365 K).

[15] Koca/Üzülmez, s. 474.

araçları veya medya yoluyla diğer iletişim araçlarıyla gerçekleştirilmesi de olanaklıdır (CGK. 13.4.1999, 9-50/61 Sayılı karar).

Tahkir edici nitelikte olup olmadığı: İsnat somut bir fiil veya olgu isnat edilmesi ya da sövme suretiyle hakaret edilmesi şeklinde gerçekleşir. İsnadın kişinin onur, şeref ve saygınlığını rencide edebilecek nitelikte olması gerekmekle birlikte, bunların gerçekten de rencide olmuş olması ve bu anlamda kişinin onur şeref veya saygınlığının zarar görmüş olması gerekmemektedir[16]. Belirtmek gerekmektedir ki hareketin bu nitelikte olup olmadığı hususunda Türk toplumunda geçerli olan ortalama örf ve adet kuralları dikkate alınacaktır. Bunun yanı sıra fiilin gerçekleştirildiği sırada geçerli olan değer yargıları da göz önünde bulundurulacaktır[17]. Fiilin tahkir edici nitelikte olup olmadığı noktasında değerlendirilmesi gereken bir diğer husus ise mağdurun sıfatı, sosyal konumu ile fiilin işlenmesi sırasındaki hal ve koşullar olarak belirlenmektedir[18]. Bunlarla birlikte Yargıtay *"AİHS ve hukuk düzenimizin koruduğu düşünce özgürlüğü kapsamında kalmayan, anlam ve içerik derinliğinden yoksun, sloganik tarzda aşağılayıcı ve hakaret kastıyla söylenmiş paylaşımlar"*ı konu edindiği bir kararında, bu türden sosyal medya paylaşımlarının da hakaret suçunun fiil unsurunu oluşturduğu neticesine varmaktadır[19]

Fiil ve olgu isnadı mı sövme mi: fiil veya olgu isnadı gerçekleşmiş belirli bir olayın veya işlenmiş bir fiilin mağdura yüklenmesini ifade etmektedir. Bunu sövmeden ayıran bir değer yargısı içermemesidir. Dolayısıyla ortada ispata konu olabilecek, doğruluğu veya yanlışlığının değerlendirmeye tabi tutulabilmesi mümkün olan somut bir olgu ya da fiilin varlığı gerekmektedir[20]. Mağdura izafe edilen fiil veya olgunun içeriği itibariyle objektif doğruluğunun sınanabilir nitelikte olması gerekmektedir.belirtmek gerekir ki şu andaki TCK düzenlemesine göre fiil veya olgu isnadı veya sövme biçimindeki hakaretler aynıceza ile cezalandırılmaktadır. Ancak hakaretin fiil/olgu isnadı veya sövme olup olmadığının belirlenmesi fail bakımından isnadı ispatının gündeme gelebilmesi açısından önem arz eder. İsnadın ispatı yalnızca fiil/olgu isnadı şeklinde gerçekleşen hakaret suçları açısından tanınmıştır.

Fiil veya olgunun somut olmasından maksat ise belirli bir fiil veya olgunun mağdura yüklendiğini gösterecek biçimde yer, zaman, konu, gerçekleşme biçimine ilişkin tamamlayıcı koşulların belirtilmesi suretiyle belirtilmesidir. Ancak yer, zaman, konu ve gerçekleşme biçimine ilişkin tüm hususların belirtilmesi zorunluluk arz etmez; bu fiil veya olguyu diğerlerinden ayırt etmeye yarayacak ölçüde bilgi sunulması yeterli görülmektedir[21]. Nitekim Yargıtay da kararlarında yer, kişi, zaman, konu ve fiilin gerçekleşme biçimi unsurlarının hepsinin isnatta bulunmasını haklı olarak aramamış, fiili belirginleştirecek kadarının yer almış olmasını somut fiil veya olgu isnadının(hakaret suçunun) varlığı için yeterli saymıştır[22].

Huzurda Hakaret: Hakaret suçunun huzurda işlenmiş sayılması için söylenen sözün herhangi bir aracıya gerek duyulmaksızın **doğrudan doğruya mağdura** hitaben sarf edilmiş ve mağdur tarafından öğrenilmiş olması gerekmektedir.

Gıyapta Hakaret: Mağdurun gıyabında gerçekleşen hakaret suçunun oluşabilmesi için mutlaka en az üç kişi ile ihtilat edilerek işlenmesi gerekmektedir**.** Kanunda ihtilatın nasıl olacağı belirlenmemiş ise de, ihtilat sözle, yazı ile, internet, sms, e-posta, radyo, telefon, televizyon

---

16 Tezcan, Erdem, Önok, Teorik ve Pratik Ceza Özel Hukuku, ONALTINCI Baskı, Seçkin, Ankara, Eylül 2018, s. 591; Centel/Zafer, Çakmut, Kişilere Karşı Suçlar, s. 236; Özbek, İzmir Şerhi, s. 866)

17 Tezcan, Erdem, Önok, Teorik ve Pratik Ceza Özel Hukuku, ONALTINCI Baskı, Seçkin, Ankara, Eylül 2018, s. 593; s. 591; Centel/Zafer, Çakmut, Kişilere Karşı Suçlar, s. 237.

18 Tezcan, Erdem, Önok, Teorik ve Pratik Ceza Özel Hukuku, ONALTINCI Baskı, Seçkin, Ankara, Eylül 2018, s. 595; Centel/Zafer, Çakmut, Kişilere Karşı Suçlar, s. 227; Özbek, İzmir Şerhi, s. 865.

19 **T.C.YARGITAY 16. CEZA DAİRESİ E. 2016/6928 K. 2017/4807 T. 19.7.2017**

20 Ayhan Önder, Şahıslara Karşı Cürümler, s. 240; Tezcan, Erdem, Önok, Teorik ve Pratik Ceza Özel Hukuku, ONALTINCI Baskı, Seçkin, Ankara, Eylül 2018, s. 595; Centel/Zafer, Çakmut, Kişilere Karşı Suçlar, s. 238; Özbek, İzmir Şerhi, s. 865.

21 Tezcan, Erdem, Önok, Teorik ve Pratik Ceza Özel Hukuku, ONALTINCI Baskı, Seçkin, Ankara, Eylül 2018, s. 595; Centel/Zafer, Çakmut, Kişilere Karşı Suçlar, s. 227; Önder, s. 240.

22 "Hasbekli Hacı, beni soydun, altınlarımı insanlık namına geri ver" (4. CD. 31.10.2007, 11657/14078); "Orospusun kaynınla yattın" (4. CD. 01.05.2006, 6218/ 8844); "Orospuluk fahişelik yapıyorsun, ikinizi de A. Başkomiser satıyor" (2. CD. 27.02.2006); "Cemalettin'in altından kalkıp geldin" (4. CD. 27.01.2004, 695/731) "N'nin M.G. ile ilişkisi var, bize yaramaz, kızınızı götürün" (4. CD. 27.05.2002, 7266/9259); "Sen PKK'lısın teröristlere yardım ve yataklık ediyorsun" (4. CD. 25.03.2002, 2405/4568); "Keçilerimi sen çaldın" (4. CD. 27.11.2000), 7859/8178)

yoluyla işlenebileceği gibi teknik gelişmeler doğrultusunda değişik erişim araçları ile de gerçekleştirilebilir[23].. İhtilat, hakarete ilişkin içeriğe en az üç kişi tarafından öğrenilmiş olunması anlamına gelmektedir. Öğrenmiş olma ihtimali bu noktada tek başına yeterli değildir, üç kişinin bunu gerçek anlamda öğrenmiş olmaları lazımdır. Nitekim ihtilat şartının gerçekleşmesi için öğrenecek olan kişilerin aynı yerde bulunma[24], birbirlerinden haberdar olmaları şart değildir[25]. Bir görüşe göre gıyapta hakaret suçunda htilat şartı, bir objektif cezalandırılabilirlik koşuludur[26]. Buna göre failin bu kişilerin hakareti öğrenmesini istemesi şart değildir[27]. Dolayısıyla en az üç kişinin hakaret içeriğinden haberdar olması durumunda failin kastı ihtilatı kapsamıyor olsa da failin hakaret suçundan cezalandırılması mümkün olur[28]. Ancak belirtmek gerekmektedir ki objektif cezalandırılabilirlik koşulları esasen failin cezalandırılabilmesini güçleştirmeyi amaçlayan koşullar olarak kabul edilmektedir. Bu noktada gıyapta hakaret suçları bakımından ihtilatın objektif cezalandırılabilirlik koşulu olarak kabul edilmesi bunun tam tersi bir etkiye sahip olacaktır. O nedenle kanaatimizce failin kastının ihtilatı da kapsaması gerekmektedir. Nitekim fail gıyapta işlenen hakaret suçları bakımından bunun üç kişi tarafından idrak edilebilme ihtimalini muhakkak veya muhtemel görmüyor yani doğrudan veya olası kastla hareket etmiyorsa bu durumda suçun oluştuğunu söylemek mümkün olmamalıdır.

Nitelikli Haller: Hakaret suçu ile ilgili birden fazla nitelikli hal öngörülmüş olmasına karşın özellikle internette gerçekleşen hakaret suçları bakımından önem arz eden nitelikli hal suçun aleni olarak işlenmesidir. Söz konusu düzenleme hakaretin alenen işlenmesi halinde cezanın altıda biri oranında arttırılacağını öngörmektedir. Aleniyet, belirsiz sayıda kişilerin hakaret içeren içeriği öğrenmelerine olanak sağlayan herhangi bir araç kullanmak suretiyle suçun işlenmesini ifade etmektedir. Bu noktada failin hakaret içeren ifadeye başka kişilerce de vakıf olunmasına ilişkin olanağı yaratmış olması yeterlidir, ifadeye fiilen ulaşılıp ulaşılamadığı nitelikli unsurun uygulanması bakımından önem arz etmez[29]. Yargıtay'a göre "*Aleniyetin gerçekleşmesi için olay yerinde başkalarının bulunması yeterli olmayıp, hakaretin belirlenemeyen sayıda kişi tarafından görülme, duyulma, algılanabilme olasılığının bulunması, herhangi bir sınırlama olmaksızın herkese açık olan yerlerde işlenmesinin gerekmesi*"[30] söz konusudur. Örneğin Yargıtay trafik kontrolünün yapıldığı karayolunu, kamuya açık parkı, cadde üzerini ve karakol binasını hakaret suçunda aleniyet unsurunun gerçekleşmesi bakımından elverişli alanlar olarak görmüştür[31]. 5237 sayılı Kanun hakaretin basın yoluyla işlenmesini nitelikli hal olarak öngörmemektedir. Ancak

---

[23] Sanığın kendisine zayıf not veren öğretim görevlisi, mağdur ile birkaç kişiye gönderdiği "e-posta" iletisiyle mağdura sövmekten ibaret eyleminde; Sözü edilen iletiyi internet servis sağlayıcısından gönderen bilgisayarın (İ.P) numarasının sorulması, bu yolla bilgisayarın kime ait olduğunun saptanması sonucuna göre; (1) İnternet kafe gibi umuma açık yerlerde bulunan bir bilgisayardan ileti gönderilmiş ise sanığın beraatine, (2) Sanığın evi ya da işyerinde bulunan kişisel bilgisayarından gönderilmiş ise mahkumiyetine, (3) Olayla ilgisi bulunmayan bir üçüncü kişinin kişisel bilgisayarından gönderilmiş ise, bu şahsın tanık olarak dinlenmesi ve sonucuna göre karar verilmesi gerekirken, eksik soruşturma sonucu yazılı biçimde hüküm kurulması, bozmayı gerektirmektedir, (Y.4.CD. 05.12.2005 T.,2004/8763 E.2005/21445 K.)

[24] Nitekim Yargıtay bir kararında, sanığın mağdurun kocasına, kayınpederine ve kayınvalidesine hitaben yazıp gönderdiği mektuplarla mağdurun gıyabında madde tayini suretiyle hakarette bulunduğunu ve ihtilat unsurunun gerçekleşmiş kabul edilmesi gerektiğini hüküm altına almıştır. 4. CD., E. 1980/2510, K. 1980/2529, T. 10.4.1980

[25] Tezcan, Erdem, Önok, Teorik ve Pratik Ceza Özel Hukuku, ONALTINCI Baskı, Seçkin, Ankara, Eylül 2018, s. 601.

[26] ÜZÜLMEZ, İlhan, "Hakaret Suçu", Ceza Hukuku Dergisi, Yıl: 5, Sayı:12, Ankara, Nisan 2010, s.53.

[27] Tezcan, Erdem, Önok, Teorik ve Pratik Ceza Özel Hukuku, ONALTINCI Baskı, Seçkin, Ankara, Eylül 2018, s. 601.

[28] Gıyapta hakaret suçunun ihtilat unsurunun oluşması için sanığın söylediği iddia olunan hakaret içerikli sözlerin ikiden çok kimse tarafından duyulması gerektiği nazara alındığında, E.G ve M.E. dışında başka kişilerce de duyulup duyulmadığı araştırılmadan eksik inceleme ile mahkumiyet kararı verilmesi (Y2CD, 16.4.2008, 17950, 7200).

[29] Tezcan, Erdem, Önok, Teorik ve Pratik Ceza Özel Hukuku, ONALTINCI Baskı, Seçkin, Ankara, Eylül 2018, s. 605; Centel/Zafer/Ççakmut, Kişilere Karşı Suçlar, s. 255; Önder, Şahıslara Karşı Suçlar, s. 246;

[30] Y9CD, 14908/8838, 8.9.2014;.

[31] Y4CD20573/18198; Y3CD, E. 2015/31078, K. 2016/11125 T3.5.2016; Y5CD 2013/14084, K. 2015/1027, 15.1.2015; Y4CD, 34/8, 16.7.2008

belirtmek gerekir ki hakaretin basın yoluyla işlenmesi halinde aleniyete ilişkin nitelikli halin uygulanması mümkündür[32]

Özellikle internette yayınlanan içerikler vasıtasıyla hakarette bu içeriklerin internet ortamında durmaları ve ulaşılabilir olmaları söz konusu olacaktır. Bu durumlarda suçun mütemadi bir nitelik kazanıp kazanmadığı önem arz eder. Suçun tamamlanması (şeklen tamamlanma) kavramı bir suç tipinde öngörülen bütün unsurların gerçekleşmesini ifade etmesine karşılık, suçun sona ermesi (madden tamamlanma) kavramı ile hukuki değerin failce istenen ölçüde ve sürece ihlal edilmesi anlamına gelmektedir. Örneğin failin mağduru öldürmesiyle kasten adam öldürme suçu tamamlanmış ve aynı anda sona ermiştir. Buna karşılık hürriyeti tahdit suçu, failin mağduru bir yere kapatması ve başka bir şekilde hareket özgürlüğünü kısıtlamasıyla tamamlanır. Ancak suç mağdurunun özgürlüğünü tekrar kazandığı anda sona erer. Suçun tamamlanması ile sona erme arasında suça iştirakin mümkün olması, zamanaşımının suçun sona erdiği andan itibaren başlaması gibi sonuçları vardır[33]. Hareketin neden olduğu neticenin belirli bir süre devam ettiği suçlara mütemadi suçlar adı verilmektedir[34]. İnternette işlenen hakaret suçlarında dagönderilen mesajların yayınlaması ile suçun tamamlandığını ancak fail bu mesajları silme iktidar ve imkanına sahip olmasına rağmen silmemiş olması durumlarında suçun halen devam ettiğini, sona ermediğini ve mütemadi bir nitelik kazandığını söylemek gerekmektedir. Gerçekten Yargıtay da internette yer alan yayınların içeriğinin bir suç teşkil etmesi durumunda bu içeriği ortadan kaldırma konusunda failin imkan ve iktidarı olup olmadığına dikkat etmektedir[35].

Hakaretin internette işlenmesinde özellik arz eden hususlar

İnternet yayınlarına ilişkin olarak 04.05.2007 tarihinde kabul edilerek 23.05.2007 tarihinde yürürlüğe giren 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun 1. Maddesinde kanunun amacını "*Bu Kanunun amaç ve kapsamı; içerik sağlayıcı, yer sağlayıcı, erişim sağla-yıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenlemektir"* şeklinde ortaya koymaktadır[36]. Hakaret suçunun internet yolu kullanılarak ve fakat yukarıda bahsettiğimiz yollar haricinde bir yolla gerçekleştirilmesi durumunda ceza sorumluluğuna ilişkin olarak bu kanunda yer alan düzenlemelerin göz önünde bulundurulması gerekecektir. Söz konusu kanun 2. Maddesinde bazı kavramların tanımına yer vermektedir. Ceza sorumluluğunun saptanabilmesi açısından bu kavramlardan özellikle içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcı kavramları özel önem arz etmektedir[37].

İnternette işlenen hakaret suçları bakımından hakaret içerikli yayının mağduru muhatap alıp almaması noktasında ayrıma gidilerek inceleme yapılması gereklidir.

İnternet aracılığıyla gönderilen elektronik posta veya mesajlar yoluyla hakaret

Bu ilk ihtimalde içerik sağlayıcı olan kişilerin doğrudan mağduru muhatap alarak bir ileti yayınlaması söz konusudur. Bunlara örnek olarak e-posta, internet bağlantısı ile mesajlaşma imkanı veren telefon uygulamaları vb verilebilir. Elektronik posta ile gönderilen veya mağdurun cep telefonuna yüklediği yazılı/sesli/görüntülü ileti göndermeye yarayan uygulamalar vasıtasıyla gönderilen ya da mağdurun üye olmak suretiyle kendisine ait bir hesabının olduğu ve mağdura ya

---

[32] Tuğrul Katoğlu, Basın Yoluyla Hakaret Kavramı ve Madde Yönünden Yetki Sorunu, Prof. Dr. Nur Centel'e Armağan, s. 737 (735-748).

[33] Kayıhan İçel/ Füsun Sokullu-Akıncı/ İzzet Özgenç/ Adem Sözüer/ Fatih S. Mahmutoplu/ Yener Ünver, İçel Suç Teorisi, İkinci Bası, İstanbul, Beta, 2000, s. 295, dn.1)

[34] İçel ve diğerleri, s. 69, dn. 78.

[35] Y9CD E. 2001/1853, K. 2001/2649 T. 25.10.2001; Ayrıca bkz: İçel ve diğerleri s. 69, dn. 78.

[36] İçel/Ünver söz konusu kanunu Basın Kanunu ile mukayese edererk Basın Kanununun bir özel ceza yasası olduğunu ve fakat 5651 sayılı kanun bakımından bunun söylenemeyeceğini, ilgili yasanın ceza sorumluluklarının belirlenmesi noktasında "yardımcı bir yasal kaynak" olduğunu belirtmektedir. (Kayıhan İçel, Yener ,Ünver, Kitle İletişim Hukuku, Beta, 2018, s. 512).

[37] Kayıhan İçel, Yener ,Ünver, Kitle İletişim Hukuku, Beta, 2018, s. 511; İçerik sağlayıcı (content provider) İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri; Yer sağlayıcı: Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri; Erişim sağlayıcı: Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri; Toplu kullanım sağlayıcı: Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayanı ifade etmektedir.

mention adı verilerek doğrudan onun da iletiyi görmesinin sağlandığı ya da doğrudan mesaj atma olanağı veren servisler yoluyla işlenen hakaret suçları bakımından TCK m. 125'te yer alan "*Fiilin mağduru muhatap alan sesli, yazılı veya görüntülü bir iletiyle işlenmesi hali"* olarak kabul edilmesi gerekmektedir. Bu durumda hakaret suçu doğrudan mağdur muhatap alınan bir iletiyle gerçekleştirilmiş olduğundan huzura eşit sayılan bir araçla işlenmiş olacağından, huzurda hakaret suçuna ilişkin genel hükümlerin uygulanması gerekmektedir. Belirtmek gerekmektedir ki doktrinde bir görüş maddenin 2. Fıkrasında yer verilen ve huzura eşit sayılan haller olarak nitelendirilen bu haller bakımından maddenin ilk fıkrasına atıf yapması nedeniyle huzurda hakaretin mi gıyapta hakaret suçunun mu oluşacağına ilişkin bir açıklık bulunmadığını belirtmektedir[38]. Ancak madde gerekçesi göz önünde bulundurulduğunda söz konusu düzenlemede huzurda hakaretin işaret edildiğinin özellikle vurgulandığı görülmektedir. Nitekim madde gerekçenin ilgili fıkraya ilişkin bölümünde "*Maddenin ikinci fıkrasında, hakaretin mağduru muhatap alan sesli, yazılı veya görüntülü bir mesajla yapılması hâlinde, birinci fıkra hükmüne istinaden cezaya hükmedileceği kabul edilmiştir. Buna göre, kişiyi muhatap alan mektup, telgraf, telefon ve benzerî araçlarla yapılan hakaret de, huzurda hakaret olarak cezalandırılmalıdır."* ifadesine yer verilmektedir. Dolayısıyla kanun koyucunun hakaretin maddenin ikinci fıkrasında yer alan hareket şekilleri ile işlenmesi durumunda huzurda hakaret suçunun oluşmasını amaçladığı açıktır. Bunun yanında kanaatimizce bu husus gerekçede belirtilmemiş olsa bile, fıkrada yer verilen tarzdaki iletilerin "mağduru muhatap alması" ifadesi de aynı sonuca ulaşılmasını gerekli kılmaktadır. Zira bir kimsenin üçüncü bir kişiyi muhatap alarak bir başkasına gönderdiği, konumuzla bağlantısı bakımından örneğin bir elektronik postada yer alan hakaret içerikli ifadeler bakımından failin kastı mağduru muhatap almak olduğundan ve fakat bunda hataya düştüğünden ve ihtilata ilişkin de bir kastı olmadığından cezalandırılamayacaktır. Bu nedenlerle söz konusu görüşe katılmak mümkün değildir.

Diğer internet yayınları aracılığıyla gerçekleştirilen hakaret fiilleri

Bir görüşe göre internetin sürekli yayın kapsamında değerlendirilmesi gerekir. Dolayısıyla internet yoluyla şerefe saldırı hali suçun basın yoluyla işlenmesi kapsamına dahildir ve yukarıda açıklanan nedenlerle huzura eşit vasıta olarak kabulü mümkün değildir.

İnternet siteleri kamuya açık birer kitle iletişim aracı olarak görülebilir mi?[39]. Bir görüşe göre haber siteleri, forumlar gibi doğrudan ve hiç bir kısıtlamaya tabi olmadan kitlelerin ulaşabileceği internet siteleri de elektronik kitle iletişim aracı olarak görülmelidir[40].

Hakaretin internet ortamında gerçekleştirilmesi yoluyla işlenmesinde bir diğer ilgili alan doğrudan mağduru muhatap almayan ve fakat internet ortamında içerik sağlayıcılar tarafından üretilmiş bulunan yayınlar aracılığıyla gerçekleştirilmesi hali olarak karşımıza çıkmaktadır. Bu durumda gazetelerin internet sitelerinde yer alan ya da başka internet sitelerinde görsel, işitsel ya da yazılı şekilde yer verilen içeriklerin Basın Kanunu kapsamında değerlendirilip değerlendirilemeyeceği tartışmalıdır[41].

İnternet yayınları kanununa göre içerik sağlayıcılar internet ortamında kullanıma sundukları her türlü yayından sorumludurlar. Böyle bir durumda örneğin bir içerik sağlayıcı olarak youtube kanalına bir video çekip yükleyen kimsenin içerik sağlayıcı olarak ceza sorumluluğu noktasında herhangi bir tereddüt bulunmamaktadır.

Hakaret suçu bakımından ise burada hakaretin ne şekilde gerçekleştirileceği içeriğin arz edildiği internet ortamına göre farklılık gösterecektir. Örneğin twitter isimli internet sitesi gibi kişilerin belirli isimler alarak üye oldukları ve birbirlerinin paylaşımlarını takip etmek suretiyle görebildikleri bir internet sitesini göz önüne aldığımızda, burada failin hakaret içerikli iletiyi üretmesi ve siteye koymasında eğer ki mağduru doğrudan *mention* yöntemi ile muhatap alarak yapmamış ise gıyapta hakaret suçunun gündeme geleceğini belirtmek gerekir. Zira burada fail ve mağdur birbirlerini takip ediyor olsalar da ortada mağduru muhatap alan bir ileti olmayacağından huzurda hakaret suçu değil gıyapta hakaret suçu gerçekleşir. Hal böyle olunca failin iletisini kaç kişinin görebileceği yani ihtilat şartının gerçekleşip gerçekleşmediği ve failin kastının ihtilatı da

---

[38] Katoğlu, s. 739.

[39] Hasan Sınar, İnternet ve Ceza Hukuku, 2001, s. 34

[40] Fehmi Şener Gülseren, İnternet Ortamında İşlenen Hakaret Suçları, EUL Journal of Social Sciences, IV:I, June 2013, s. 19 (15-33)

[41] Katoğlu, s. 739.

kapsayıp kapsamadığı meselesi gündeme gelir. Buradaki bir diğer sorun yine üye olunarak kullanıma imkan sağlayan sosyal medya platformlarında (örneğin facebook, twitter gibi) fail ve mağdurun birbirini takip etmesi gibi durumlarda failin mağdura yönelik bir hakaret suçunu işlemiş olmasında fakat mention vermemesi durumunda gıyapta hakaretin mi huzurda hakaretin mi gerçekleşmiş sayılacağına ilişkin bir tartışmadır. Bu durumda failin hakaret içerikli iletisini mağdurun görmesi muhakkak değil ve fakat muhtemeldir. Hakaret suçu olası kastla da işlenebileceğinden olası kastla işlenen huzurda hakaret suçunun varlığının söz konusu olup olmadığı önem arz eder. Burada dikkat edilmesi gereken husus ileti yoluyla yapılan hakaretlerde iletinin mağduru muhatap almasıdır. Dolayısıyla bu gibi durumlarda mağduru muhatap alan bir iletiden söz edilmeyeceğinden söz konusu durumda gıyapta hakaret hükümlerine gidilmesi gerekecektir. bu ihtimalde de gıyapta hakaretin oluşması için gerekli olan ihtilat şartının hukuki niteliği önem arz eder. Eğer failin hakaret içerikli iletisini üç veya daha fazla kişinin görmesi konusunda kastı varsa bu durumda gıyapta hakaret suçu gerçekleşmiş olur. Ancak örneğin twitterda failin örneğin mağdurla birlikte toplam üç takipçisi varsa ve failin bu hesabı herkesin görebileceği şekilde açık bir hesap değilse bu durumda ihtilat şartı gerçekleşmiş olmayacağından hakaret suçu oluşmayacaktır.

Burada özel önem arz eden iki tartışmalı husus bulunmaktadır. Bunlardan ilki maddede içerik sağlayıcıların sorumluluklarının belirlenmesinde göz önünde bulundurulması gereken ve "*içerik sağlayıcı bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak sunuş biçiminden bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise genel hükümlere göre sorumludur*" şeklindeki düzenlemedir. Burada özellikle iştirak bakımından sorunlar ortaya çıkmaktadır.

Bir diğer önemli husus ise internette yer alan haber siteleri, gazetelerin internet sayfaları gibi yayınlar bakımından Basın Kanunun mu yoksa ilgili kanunun mu uygulanacağı olacaktır. Kanaatimizce bu gibi yayınlarda Basın Kanunun uygulanma bulma imkanı bulunmamaktadır.

Diğer bir tartışmalı husus ise iftira suçunun gerçekleşme biçiminden biri olan basın yayın yoluyla işlenmesi halinde internet yayınlarının da bu kapsamda olup olmadığıdır. İnternet yayınları TCK m. 6 uyarınca basın yayın yoluyla işlenmesi kapsamına dahildir. Dolayısıyla basın yayın yoluyla yapılan bir fiil isnadı halinde bunun hakaret mi iftira suçunu mu oluşturduğu hususu özel önem arz etmektedir. gözden uzak tutulmamalıdır.

YAPAY ZEKÂNIN CEZA MUHAKEMESİNDEKİ ROLÜ VE GELECEĞİ

Zafer İçer[*]

Başak Buluz[**]

Özet

İçinde bulunduğumuz yüzyılın başlarından itibaren inovatif teknolojiler benzerine rastlanmamış hızla gelişerek yayılmış; siber-fiziksel sistemler ve bu sistemleri birbirine bağlayan internet yoluyla ortaya konulan yenilikler, teknoloji çağını doğurmuştur. "Sanayide Dijital Dönüşüm" olarak da adlandırılan bu devrimin katalizörü olarak görülen yeni teknoloji çağının en önemli öznelerinden biri de şüphesiz yapay zekâ sistemleridir. Birçok farklı disiplinle etkileşim içerisinde olup sürücüsüz araçlardan, sanal asistanlara; akıllı ev ürünlerinden sanayi otomasyonlarına kadar her noktada insanlığa ve gündelik hayata temas eden yapay zekâ sistemleri, son dönemde tüm hukuk sahasında olduğu gibi ceza muhakemesinde de yerini almaya başlamıştır. Muhtelif ülkelerde, somut hukuki ihtilafları tanımlayıp analiz ederek açılacak davaların olası sonuçlarını tahmin eden akıllı dijital asistanlar aktif kullanıma girmiş; hukuki analiz ve delil değerlendirmesi gibi hususlarda yapay zekâ platformlarından faydalanılmaya başlanmıştır. Hiç şüphesiz, bu sistemlerin ortak hedefi bu alanda, hızlı, verimli ve doğru çözümler ortaya koymaktır. Diğer yandan yakın gelecekte robotik sistemlerin bizzat yargılamanın süjesi hâline gelmesi, robot hâkim, savcı ve avukatlara karar alma süreçlerinde önemli roller yüklenmesi de kuvvetle muhtemel görünmektedir. Bu çalışmada yapay öğrenme ve yapay zekâya ilişkin teknik hususlara da değinilmek suretiyle söz konusu bu akıllı sistemlerin ceza muhakemesindeki rolü ve geleceği, mevcut örnekler ve olası gelişmeler ışığında bilimsel bir perspektifle ele alınacaktır.

Anahtar Kelimeler: *yapay zeka, ceza muhakemesi hukuku, bilişim hukuku.*

THE ROLE AND FUTURE OF ARTIFICIAL INTELLIGENCE IN CRIMINAL PROCEDURE LAW

Abstract

Since the beginning of the present century, innovative technologies have evolved with unprecedented speed; cyber-physical systems and the innovations which produced through the

[*] Dr. Öğr. Üyesi, Marmara Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku (zafericer@marmara.edu.tr)

[**] Öğr. Gör. Yüksek Mühendis, İstanbul Aydın Üniversitesi ABMYO (İng.) Bilgisayar Programcılığı (basakbuluz@aydin.edu.tr)

internet linking these systems have created technological era. One of the most important subjects of the digital era is "artificial intelligence systems" what called the catalyzer of industrial digital transformation of course. Artificial intelligence systems are interact with many different disciplines and that touch humanity and everyday life at any point from driveless cars to virtual assistants, from smart home products to industrial automation; and in recent years, as in all legal fields, it has began to take its place in Criminal Procedure. In various countries, intelligent digital assistants have been actively used to identify and analyze concrete legal conflicts and predict the possible consequences of the lawsuits to be opened and artificial intelligence platforms are being used in subjects such as legal analysis and evidence evaluation. Undoubtedly, the common goal of these systems is to provide fast, efficient and accurate solutions in this area. On the other hand, in the near future, robotic systems are likely to become the subjects of judging and they may have important roles in decision-making processes as robot judges, prosecutors and lawyers. In this study, the role and future of these intelligent systems in criminal proceedings will be discussed with a scientific perspective in light of current examples and possible developments by referring to technical aspects of artificial learning and artificial intelligence.
***Keywords:**, artificial intelligence, criminal procedure law, information and technology law.*

I. GİRİŞ, YAPAY ZEKA VE HUKUK İLİŞKİSİ

1950 yılında Alan Turing tarafından yayınlanan "Computing Machinery and Intelligence" isimli makalede[1] "Makineler düşünebilir mi?" ("Can machines think?") sorusu ile başladığı varsayılan yapay zeka konulu tartışmalar, hukuk alanında aslında bu sorudan yaklaşık 277 yıl öncesinde tartışılmaya başlanmıştır. Dört işlem yapabilen makine icadıyla, adı matematik alanında sıkça duyulan ancak aslında hukuk mezunu olan Gottfried Wilhelm Leibniz, muhakemelerin matematiksel olarak hesaplanabilmesinin kişilerarası anlaşmazlıkların çözümü olduğunu savunarak, bugün hukuki yönünü tartıştığımız "robot yargıç" yapısının hayalini 17. yüzyılda kurmaya başlamıştır.

"Yapay zeka (YZ)" kavramının literatüre kazandırılması 1956 yılında Dartmouth Koleji tarafından düzenlenen Dartmouth Konferansı'na dayanmaktadır. Massachusetts Teknoloji Enstitüsü (MIT) YZ Laboratuvarı'nın kurucusu Marvin Minsky, Amerikan YZ Derneği'nin ilk başkanı Allen Newell gibi alanın öncülerinden kabul edilen yaklaşık 20 araştırmacı, 8 hafta süren konferansta bu alanla ilintili tüm araştırma alanlarını kapsayan, nötral bir isim bulmayı amaçlayarak bir araya gelmiştir.

---

[1] Turing, A. M. (2009). Computing machinery and intelligence. In *Parsing the Turing Test* (pp. 23-65). Springer, Dordrecht.

YZ kavramının isim babası olarak kabul edilen John McCarthy "özellikle akıllı bilgisayar programları başta olmak üzere akıllı makineler üretme bilimi ve mühendisliğidir" şeklinde bir yapay zeka tanım yapmışsa da[2], bu kavramın literatüre kazandırılmasından bu yana 60 yılı aşkın zaman geçmesine karşın herkes tarafından kabul görmüş tek bir tanımın mevcudiyetinden bahsetmek mümkün değildir.

Henüz tanımı konusunda dahi mutabık kalınamayan bu teknolojik evrilme dünya ülkeleri tarafından bir devrim olarak kabul edilmiştir. Ülkemizde de "Sanayide Dijital Devrim" ismi ile anılan ve dördüncü sanayi devriminin çıkış noktası kabul edilen gelişim ve dönüşüm süreci meslekler, kavramlar ve insan yaşamı içerisine dahil olan hemen her noktada etkisini süratle göstermeye devam etmektedir.

Bu minvalde hukuk alanında da gerek YZ altyapısı ile desteklenmiş ürün ve uygulamaların kullanımına bağlı olarak meslek erbaplarının iş rutinlerinde köklü değişimlere sebep olması yönüyle; gerekse hukuk alanında olduğu gibi diğer çalışma alanlarında da yerini alan ve akıllı diye tabir edilen ürünlerin kullanımından doğan zafiyetlerde hukuki sorumluluklarının belirlenmesi açısından YZ, üzerinde durulması zorunlu bir konu haline gelmiştir.

Sıklıkla metin verileri üzerinde çalışmayı gerektiren hukuk alanı, YZ'nın güçlü bir çalışma alanı olan Doğal Dil İşleme'nin (DDİ) konusu dahilinde ele alınmayı gerektirmektedir. Yakın vadede iş rutinlerinde kolaylık sağlayan ve meslek süreçlerini büyük ölçüde değiştiren yardımcı uygulamaları ile alana katkı sağlarken, uzun vadede yargı süreçlerinin karar destek sistemleri ile destekleneceği öngörülmektedir.

II. YAPAY ZEKA UYGULAMALARINA TEMEL OLUŞTURAN DOĞAL DİL İŞLEME

Dil, toplumların geçmişinden gelen ve geleceğine taşınan; o toplumun yaşayış biçimi, kültürü ve tarihini en iyi yansıtan varlıktır. Ortak bir dil benimseyerek iletişim kuran toplum bireylerini etkileyen tüm kültürel, siyasi ve sosyal olaylar kadar etkisinde kalınan diğer toplumlar da bir dilin gelişim ve değişimi üzerinde etki yaratırlar. Bu etki, dilin yaşayan bir varlık olduğunun ispatı niteliğindedir.

İnsanlığın gelişimindeki kilit adımların birçoğu dil kullanımı ve ardından yazı yoluyla iletişim kurulması sonrasında atılmıştır. Kendini diğer varlıklardan düşünme yeteneği ile ayıran insanların, öncelikle kendini anlama ve ardından da kendi gibi düşünen ve davranan araçlarla

[2] McCarthy J., What is artificial intelligence? Computer Science Department, Stanford University. Available from: http://www-formal.stanford.edu/jmc/whatisai.pdf (e.t.:20.08.2019)

birlikte yaşamını devam ettirme istediğinden doğan YZ'nın konusu dahilinde doğal dili anlamanın var olması da kaçınılmaz bir sonuç olarak ortaya çıkmıştır.

Doğal Dil İşleme (DDİ) konusu dahiline giren çalışmalar dil bilimden beslenerek, işlenecek dil için en küçük anlamdan söz dizimine ve ardından anlam bütünlüğüne kadar uzanan bilimsel bir çalışmayı gerektirir. Dil bilim ve istatistik biliminin birlikteliği ile dilin matematiksel ifadelere dönüşümü sağlanır. Bu sistematik yapı "Hesaplamalı Dil Bilim" diğer bir deyişle "İstatistiksel Doğal Dil İşleme" olarak isimlendirilir. Genel manada Doğal Dil İşleme ise, temelde doğal dilde oluşturulmuş metin ve ses gibi girdilerin dil bilimi ve hesaplamalı dil bilimin ışığında makine öğrenmesi yöntemleri ile işlenmesi ve duygu analizi, metin özetleme, bir dilden diğer bir dile çeviri yapılması, metinden bilgi çıkarımı, soru cevaplama gibi insanlar tarafından kimi zaman içgüdüsel kimi zaman ise uğraşlar sonucu gerçekleştirilebilen görevlerin makineler tarafından otomatik olarak yapılması olarak ifade edilebilir.

Doğal dil ile iletişim kurmak için temelde metinler ve seslerden faydalanılmasından hareketle, bu iki temel kaynağın oluşturduğu tüm haber metinleri, reklamlar, e-postalar, sesli mesajlar gibi çıktılar DDİ için üzerinde çalışılacak materyaller olarak görülürken, hukuk perspektifinden bakıldığında bu materyaller dava dosyaları, kanun maddeleri, vb. gibi çoğu zaman metinlerle ifade edilen bir alanı kapsar.

III. HUKUK ALANINDA DOĞAL DİL İŞLEME UYGULAMALARI

Dijital çağın dönüştürücü etkisi hemen her alanda olduğu gibi hukuk alanında da kavramsal yenilikleri ve yenilikçi uygulamaları beraberinde getirmiştir. Bu etki sonucunda ortaya çıkan "legal tech" (hukuk teknolojisi) kavramı alanda yerini almakla beraber, üzerine kitap yazılacak niteliğe ulaşmıştır[3]. İleri teknoloji döneminin bir getirisi olarak yerini günden güne sağlamlaştıran hukuk teknolojileri, önceleri bürokratik süreçleri kolaylaştıran daktilo, telefon, teleks, faks, telsiz telefon, fotokopi, çağrı cihazı ve bilgisayar gibi araçlarla yalnızca iç paydaşların iş yüklerini hafifletirken; bugün (hali hazırda ülkemizde kullanılan UYAP[4], SEGBİS[5], ARYA[6], HUKUK

[3] Hartung, M., Bues, M. M., & Halbleib, G. (2017). *Legal Tech*. CH Beck.

[4] UYAP; günümüzün gerekli tüm teknolojik gelişmelerini kullanarak, Adalet Bakanlığı merkez ve taşra teşkilatının, bağlı ve ilgili kuruluşlarının, adli ve idari tüm yargı ve yargı destek birimlerinin donanım ve yazılım olarak iç otomasyonunu ve benzer şekilde bilgi otomasyonu sistemlerini kurmuş kamu kurum ve kuruluşları ile dış birim entegrasyonunu sağlayan ve e-Dönüşüm sürecinde e-Adalet ayağını oluşturan bir bilişim sistemidir. Bkz. https://www.uyap.gov.tr/MSayfalar.aspx?Git=Genel-Bilgi

[5] Ceza Muhakemesinde Ses Ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmeliğin (RG: 20.09.2011, 28060) 3 üncü maddesinde SEGBİS, UYAP Bilişim Sisteminde ses ve görüntünün aynı anda elektronik ortamda iletildiği, kaydedildiği ve saklandığı Ses ve Görüntü Bilişim Sistemi olarak tanımlanmıştır.

[6] https://www.webtekno.com/turkiye-deki-yargitay-davalarini-dogru-tahmin-eden-yapay-zeka-gelistirildi-h58904.html (e.t.: 30.09.2019)

WORK[7], TURKLEX[8] sistemleri gibi) yalnızca iç paydaşların iş yükünü hafifletmekle sınırlı kalmayıp, dış paydaşların da herhangi bir üçüncü kişiye ihtiyaç duymaksızın hukuki süreçler hakkında bilgi edinebilmesine ve basit hukuksal sorunlarına çözüm üretilebilmesine olanak sağlamaktadır.

Yeni nesil teknolojiler, yapay zeka çağının gerekliliği olarak veriden öğrenen sistemler olarak karşımıza çıkmaktadır. Konu, hukuk teknolojileri özelinde ele alındığında çoğunlukla öğrenilecek ve işlenecek verilerin kanun maddeleri, dava dosyaları benzeri doğal dilde yazılmış metinlerden oluştuğu bilinmektedir. Bu noktada YZ'nın çalışma kollarından biri olan Doğal Dil İşleme devreye girmektedir. Bugün temel iş süreçlerini, avukatlık ortaklık yapısını, istihdam oranlarını ciddi oranda değiştirmeye başlayan ve artık ceza muhakemesinde karar destek sistemleri ile başarılı örneklerine rastlanan DDİ uygulamaları hukuk alanında kullanılmaya başlanmıştır.

Günümüzde kullanılan Doğal Dil İşleme temelli hukuk teknolojilerini kullanımlarına göre 5 temel başlık altında toplayabilmek mümkündür:

1. Vekillik Görevinin Özenli Şekilde İfasına Yönelik Yardımcı Uygulamalar (Due Diligence)

Avukatların görevini dikkat ve özenle yerine getirme yükümlülüğü kapsamında değerlendirilen somut görünüm biçimleri; avukatın mevzuatı bilme ve değişiklikleri takip etme, yabancı hukuka ilişkin özen, yargısal kararlara ilişkin özen, öğretiyi takip etme, adli yardıma ilişkin özen, yardımcı elemanın seçimi ve çalışmalarına ilişkin özen, avukatın bir başkasını tevkil etmesi durumunda özen, talimatları zamanında yerine getirme ve talimat almadan iş yapmama, büro organizasyonuna ilişkin özen, müvekkile ait paraları ve değerli şeyleri gecikmeksizin müvekkile bildirme ve verme, avukatın üstlenmiş olduğu iş ile ilgili gelişmelerden müvekkilini haberdar etme, kanuni yollara zamanında başvurma ve gereksiz başvuru yapmama ve dosya tutma ve belgeleri dosyalama yükümlülüklerini kapsar[9].

Bu yükümlülüklerin yerine getirilmesine yönelik DDİ temelli yardımcı uygulamalardan biri olan *Kira Systems*[10] sözleşmelerde yer alan kilit sorunların ve bilgilerin otomatik tespitinin yapılması, davayı takip eden ekibin tüm inceleme sürecinin baştan sona düzenlenmesi, yürütülen dava

---

7 https://www.hukukmedeniyeti.org/haber/20192/hukuk-bilgi-sistemi-hukuk-work-yay-n-hayat-na-ba-l/ (e.t.:30.09.2019)

8 https://www.turklex.com/hukuki-analiz/ (e.t.: 30.09.2019)

9 Akil C., "Türkiye Barolar Birliği Disiplin Kurulu Kararları Işığında Avukatın Görevini Özenle Yerine Getirme Yükümlülüğü Araştırma". *Hacettepe Hukuk Fakültesi Dergisi*, *2*(1), (2012), 11-26.

10 https://kirasystems.com/ (e.t.:20.08.2019)

süreçlerinin özetinin bir bakışta sunulması gibi birçok işlevi içinde barındıran ve ilk kez kullananlar için %40, deneyimli kullanıcılar için %90 oranında zaman tasarrufu sağlayan bir yazılımdır.

Kira Systems'e oranla daha kısıtlı uygulama alanı sunan, ancak farklı formatlarda bulunan hukuki metinlerden bilgilerin otomatik olarak çıkarılması, yapılandırılmış veriye dönüştürülmesi ve dolayısıyla kolaylıkla raporlama yapılabilmesi konusunda büyük kolaylık sağlayan *LEVERTON*[11], bulut tabanlı yapısı ile 20'den fazla farklı dil için yüksek hızda işlem yapabilmektedir.

2017 yılının Ağustos ayı itibari ile Asya, Avrupa ve Kuzey Amerika'daki 11 hukuk bürosunda kullanıma sunulan 50'den fazla belgeyi bir dakikadan daha az bir sürede, manuel inceleme sürecinden %10 daha doğru analiz edebildiği iddia edilen *eBrevia*[12], sözleşmelerden bilgi çıkarımı ve sözleşmelerin analizi konusunda avukatlara yardımcı olmaktadır.

Avukatların ancak 360.000 saatte gerçekleştirebilmesi mümkün olan iş yükünü saniyeler içinde tamamlama kapasitesiyle adını duyuran *COIN* isimli yazılım, bankaların yılda ortalama 12.000'in üzerinde işlediği kredi sözleşmelerinin insana oranla daha doğru ve hızlı şekilde işlenmesini sağlamak üzere tasarlanmıştır [13].

Standford Üniversitesi ve Duke Kaliforniya Üniversitesi'nden 20 hukuk profesörüne karşı, sözleşmelerdeki 30 hukuki sorunun tespit edilmesi görevi için karşı karşıya gelen *LawGeex* isimli YZ yazılımı, avukatların 4 saat harcayarak %85 doğruluk oranında tespit edebildiği hukuki sorunları yalnızca 26 dakikada %95 doğruluk oranı ile tespit edebilmiştir[14].

Amerika'nın en büyük dolandırıcılık davası olan Bernie Madoff davasında kısmen kullanıldığı bilinen *ROSS Intelligence*, doğal dilde sorulan hukuki sorulara milyarlarca belge arasından ilgili kaynakları bularak hızlı öngörü sağlanmasına olanak tanımaktadır.

2. Tahmin Teknolojisi

Dava sonucunun öngörülmesi, özellikle dava stratejilerinin belirlenmesi konusunda yol gösterici bir rehber niteliğindedir. Bu öngörüye sahip olabilmek, uzun yıllara dayanan mesleki deneyim

---

11 https://www.leverton.ai/ (e.t.:20.08.2019)

12 https://www.bloomberg.com/news/articles/2017-02-28/jpmorgan-marshals-an-army-of-developers-to-automate-high-finance (e.t.:20.08.2019)

13 Bkz. dip.9.

14 https://www.lawgeex.com/resources/aivslawyer/ (e.t.:20.08.2019)

gerektirir. İhtiyaç duyulan bu deneyim YZ teknolojisi çerçevesinde verilerden elde edilebilmektedir.

2004 yılında Washington Üniversitesi'nden bir grup profesör, 2002 yılında görülen 628 dava için verilen Yüksek Mahkeme kararlarını tahmin etmek üzere geliştirdikleri algoritma ile uzmanların %59 oranında doğru tahmin ettiği dava sonucuna karşın %75 doğruluk oranı ile uzmanları geride bırakan bir başarıya erişmişlerdir[15].

2017 yılında gerçekleştirilen bir diğer çalışmada ise, 1816-2015 yılları arasındaki ABD Yüksek Mahkemesi tarafından verilen 240.000'den fazla yargıç oyu (justice votes) ve 28.000 dava sonucu tahmin edilmeye çalışılmıştır. Dava sonucu tahmininde %70,2 ve yargıç oyu tahmininde ise %71,9 oranında başarılı sağlanmıştır[16].

Avrupa İnsan Hakları Mahkemesi tarafından yargılanan davaların yalnızca metin içeriğine dayalı olarak, insan hakları sözleşmesinin bir maddesinin ihlal edilip edilmediğine dair ikili bir sınıflandırma yapılması üzerinde durulmuştur. Bir metin sınıflandırma örneği olan bu çalışmada %79 oranında yüksek bir başarım elde edilmiştir[17].

Yapılan çalışmalar yalnızca akademik makalelerle sınırlı olmayıp, hukuk bürolarının rahatlıkla kullanabileceği ticari ürünlere de dönüşmüştür. Bunlardan biri, şirketlere yönelik açılan davaların azaltılmasına ve mümkün olduğunca engellenmesine yönelik geliştirilen ve e-postaların işlenmesi yoluyla risk taşıyan e-postaların otomatik belirlenerek kurumun hukuk işleri çalışanları tarafından önleyici faaliyetlerde bulunmasını sağlayan *Intraspexion* isimli yazılımdır[18]. Bu yazılım sayesinde kurumların hukuk danışmanlarının incelemek ve risk faktörü taşıyıp taşımadığını belirlemek durumunda olduğu yaklaşık 93.023 e-posta yerine, bu sayı 117'e kadar düşürülmektedir.

Hakim kararının öngörülmesi, dava dosyasına ilişkin kanun maddelerinin otomatikman belirlenmesi gibi dava stratejisinin oluşturulmasında avukatlara büyük yardımı dokunan bir yazılım olan *Ravel Law* ise 2012 yılında Standford Üniversitesi Hukuk ve Bilgisayar Bilimleri ekiplerinin bir araya gelmesi ile geliştirilmiştir[19].

---

15 Ruger, T. W., Kim, P. T., Martin, A. D., & Quinn, K. M. (2004). The Supreme Court forecasting project: Legal and political science approaches to predicting Supreme Court decisionmaking. *Columbia Law Review*, 1150-1210.

16 Katz, D. M., Bommarito II, M. J., & Blackman, J. (2017). A general approach for predicting the behavior of the Supreme Court of the United States. *PloS one*, *12* (4), e0174698.

17 Aletras, N., Tsarapatsanis, D., Preoţiuc-Pietro, D., & Lampos, V. (2016). Predicting judicial decisions of the European Court of Human Rights: A natural language processing perspective. *PeerJ Computer Science*, *2*, e93.

18 https://intraspexion.com (e.t.:20.08.2019)

19 http://ravellaw.com (20.08.2019)

İlk aşamada fikri mülkiyet konusuna odaklanan *Lex Machine,* 32 milyondan fazla Federal US Docket girdisinin temizlenmesi, etiketlenmesi ve işlenmesi ile eğitilen bir hukuk analitiği platformudur. Bu platform hakim ve mahkemelerin analiz edilmesine, muhalif avukatın daha önceki tecrübelerinin raporlanmasına, dava sürecindeki her bir adımın tahmini olarak tamamlanma süresinin çıkartılmasına, davayı kazanmaya yönelik stratejinin önerilmesine olanak sağlayan ve bu işlemlerin hemen hepsini dakikalar içerisinde tamamlayan, avukatlar için rehber niteliğinde bir DDİ uygulamasıdır [20].

Dünyanın en büyük dava veritabanına sahip olduğu iddia edilen *Premonition* yazılımı ise davanın kazanılabilme oranını, dava süresini ve türünü, hakim ile eşleştirmesini analiz ederek bir avukatın başarısını ön görebileceğini iddia etmektedir[21].

3. Hukuksal Analitik

Hukuksal analitik, avukatların daha önceki dava kazanma/kaybetme geçmişine, önceki emsal kararlara ve hakimin geçmişine dayanarak dava stratejisi hazırlığında kullanılabilecek veri noktalarının belirlenmesini ifade eder. Bu görev için kullanılan uygulamalar genellikle tahminleme teknolojisi için geliştirilen yazılımların içerisindeki modüller aracılığı ile gerçekleştirilir. *Lex Machina* ve *Ravel Law* bu amaçla kullanılan yazılımlar arasından en çok tercih edilenlerdendir.

4. Belge Otomasyonu

Veri girişi adımında doldurulması gereken belgeleri otomatik oluşturmak için oluşturulan yazılım şablonları hukuk firmaları tarafından sıkça kullanılan yazılımlardandır. İnsan gücü ile doldurulması ve hazırlanması günlerce sürebilecek bürokratik belgelendirme sürecinin hızlandırılması, iç paydaşların dava üzerinde daha yoğun zaman harcayabilmeleri için zaman kazancına dönüşmektedir.

Kullanıcıya yöneltilen sorular ve alınan cevaplara bağlı olarak, ihtiyaç duyulan belge şablonunu öneren *PerfectNDA*[22] özellikle gizlilik sözleşmelerinin oluşturulması hususunda oldukça başarılı sonuçlar sunan bir belge otomasyon yazılımıdır.

5. Fikri Mülkiyet

---

20 https://lexmachina.com (e.t.:20.08.2019)
21 https://premonition.ai (e.t.:20.08.2019)
22 https://www.neotalogic.com/product/perfectnda/ (e.t.:20.08.2019)

Patentleri, telif haklarını ve ticari markaları güvence altına almak kadar patent, marka tescil başvurusu yapmak, telif sözleşmesi hazırlamak, son derece dikkat gerektiren, uzun zaman alan ve karmaşık araştırmaların yapılmasını icap eden ve çoğu zaman bir avukatın uzmanlığına ihtiyaç duyulan süreçlerdir. Bir yazılım kullanılmaksızın yapılan bir marka ve patent araştırması, elle yapılan yüzlerce aramanın sonucuna bakmayı gerektirir. İş gücü ve zaman karmaşıklığı oldukça yüksek olan bu işlemlerin daha hızlı bir şekilde gerçekleştirilebilmesi noktasında da şüphesiz ki YZ yazılımlarından destek almak en akılcı çözümlerden biridir.

Bir avukat tarafından 1 haftada tamamlanabilecek tescilli ürünler ve ticari markalar araştırmasını 15 saniye gibi kısa bir sürede tamamlayabilme kapasitesine sahip olan *TrademarkNow* isimli yazılım, elde edilen sonuçları değerlendirerek alaka düzeyine göre sıralar ve kullanıcıya en ideal sonuç raporunu ulaştırır[23].

Patent başvurusunun yapılması esnasında yardımcı araç olarak kullanılan, bulut bilişim tabanlı olarak çalışan *Anaqua Studio*, TrademartNow benzeri işlevlerle zaman tasarrufu sağlamasının yanı sıra dokümandaki hataların otomatik tespit edilmesi ve biçimsel olarak düzenlemenin yapılması konularında da yardımcı olmaktadır[24].

Diğer taraftan *SmartShell* isimli YZ yazılımı, gerçekleştirilen bir vaka çalışmasında bir patent başvurusu için iki yardımcı avukatın birlikte yürüttükleri belgenin alınması, bibliyografik veri araştırmasının tamamlanması, denetçinin incelemesinde ortaya çıkabilecek sorunların keşfedilmesi ve reddedilme olasılığının tespit edilmesi süreçlerinin tamamında toplamda %500 ile %800 daha yüksek verimle sonuç üretebilmiştir[25].

IV. YAPAY ZEKANIN CEZA MUHAKEMESİNDEKİ ROLÜ VE GELECEĞİNE İLİŞKİN ÖNGÖRÜLER

1. Suçun Önlenmesi ve Güvenliğin Sağlanmasına Yönelik Uygulamalar

Ceza hukukunda, suça ilişkin icra hareketleri başlamadan önceki alan "hazırlık evresi" olup hazırlık hareketleri kural olarak cezalandırılabilir değildir. Elverişli hareketlerle doğrudan doğruya icraya başlandığı anda teşebbüs safhasına giriş yapılmış ve bu aşamadan itibaren fiil

---

23 https://www.trademarknow.com/ (e.t.:20.08.2019)
24 https://www.anaqua.com/corporate/products/anaqua-studio(e.t.: 20.08.2019)
25 https://turbopatent.com/smartshell/ (e.t.: 20.08.2019)

cezalandırılabilir bir hal almış olur. Böyle durumlarda failin suça teşebbüsten dolayı sorumluluğuna gidilir (TCK m.35)[26].

Ceza muhakemesi, suç işlendikten sonra başlayan ve bir dizi faaliyetten oluşan bir süreçtir. Bu süreçteki işlemler adli nitelikte iken, suçun işlenmesinin önlenmesi idari bir nitelik arz ettiğinden, suçun önlenmesine ilişkin faaliyetler idarenin görev ve sorumluluğundadır. Suçun işlenmesinden önce ceza muhakemesi faaliyeti henüz başlamadığından, önleyici faaliyetlerin yerine getirilmesi prensip olarak idarenin yetki sahasındadır.

Günümüzde ülkeler, suç öncesi alanda devletin etkinliğin artırılması yönünde bir eğilim göstermektedir. Bunun sebebi, suç işlendikten sonra, suçun etkilerinin hiçbir zaman tam manasıyla telafi edilebilir olmamasıdır. Suçun mağduru ister somut bir kişi, ister kamu isterse devlet olsun, işlenmiş bir suç, kamu düzeni ve toplum barışını bozar ya da en azından tehlikeye uğratır. Bireylerin ve toplumun hak ve menfaatlerinin etkin bir şekilde korunabilmesi, kamu düzeninin tesisi ancak suç teşkil eden fiillerin önüne geçilmesi ile mümkün olabilmektedir. Hiç şüphesiz hukuk ve ceza adalet sistemleri, suç işlendikten sonraki sürece ilişkin birtakım kurallar koyar ve muhakeme prosedürü geliştirir. Bunun sonucunda da suç işlediği sabit görülen kişiler hakkında belirli yaptırımlar tatbik edilir.

Son yıllarda, güvenlik alanında ve suçun önlenmesine ilişkin faaliyetlerde, yapay zeka uygulamalarının giderek yaygınlık kazanmaya başladığı gözlemlenmektedir.
Bu uygulamalara örnek olarak Çin'de, trafik düzeninin sağlanması ve suçluların yakalanmasına yönelik, bütünüyle yapay zeka tarafından yönetilen bir polis istasyonu geliştirilmiştir. Güvenlik kameralarıyla donatılan pek çok bölgede, yüz tanıma teknolojisi sayesinde suçluların ya da trafik ihlali yapanların tespit edilerek yakalanması amaçlanmaktadır[27].

Dubai'de ise, emniyet yetkilileri tarafından ilk robot polis kamuoyuna tanıtılarak göreve başladığı duyurulmuştur. Yetkililer, insanların robot polise suç ihbarında bulunabileceklerini, ceza ödeyebilecekleri ve üzerindeki dokunmatik ekran sayesinde ihtiyaç duydukları bilgileri alabileceklerini belirtmişlerdir[28].

---

[26] Sözüer A., Suça Teşebbüs, İstanbul 1994, s.194 vd.; İçer Z., Suça Teşebbüste Hazırlık Hareketleri İle İcra Hareketlerinin Birbirinden Ayrılması Meselesi", Marmara Üniversitesi Sosyal Bilimler Enstitüsü, (Yayınlanmamış Doktora Tezi), İstanbul 2017, s.21, 22.

[27] https://www.log.com.tr/cin-yapay-zeka-tarafindan-yonetilen-insansiz-polis-istasyonu-hazirliginda/ (e.t.:04.10.2019)

[28] https://www.bbc.com/turkce/haberler-40038611 (e.t.: 04.10.2019)

Bu alandaki uygulamaların en çarpıcı örneğini yüz tanıma teknolojileri oluşturmaktadır. Bilhassa bu teknoloji, kamusal alanlarda, meydanlarda, caddelerde bireylerin yoğun olarak geçtikleri bölgelerde konumlandırılan yüksek çözünürlüklü kamerlar aracılığıyla işlevsellik kazanmakta ve bu sayede suçların önlenmesi ve şüphelilerin tespit edilmesi amaçlanmaktadır.

Yüz tanıma teknolojisini hayata geçiren ülkelerin başında İngiltere gelmektedir. İngiltere'de *WeSee* firması yapay zeka teknolojisiyle, insanların gözünden kaçabilecek ayrıntıları yakalayarak şüpheli kişileri yüz ifadelerinden tespit edebilen bir teknoloji geliştirmiştir. Şirket yetkilileri, şüpheli kişilerin ifadeleri ve yüzlerini veri kaynağı alarak yüksek çözünürlüklü kameralar kullanmak suretiyle insanların duruşlarından, jest ve mimiklerinden, duygu durumu tespiti yapılmasının ve niyetlerinin okunmasının amaçlandığını (niyet okuma teknolojisi) belirterek, böylelikle şüpheli davranışları belirleyip suçun işlenmesinin önüne geçilebileceğini, örneğin metro istasyonuna yerleştirilen kameralar sayesinde terörist saldırı potansiyeli bulunan bir kişi tespit edildiğinde durumun hemen polise haber verilebileceğini dile getirmişlerdir[29].

Yine İngiltere'de, West Midlands bölgesindeki polis teşkilatının, ciddi şiddet içeren suçları önceden tahmin edip meydana gelmeden durdurulması amacıyla yeni bir yapay zeka yazılımının üzerinde çalıştığı basına yansımıştır. *Ulusal Veri Analiz Çözümü (NDAS)* adı verilen yazılım sayesinde polis, bir kişinin potansiyel suç işleme durumunu eldeki veriler ve istatistiklerle saptayabilmeyi ve böylelikle henüz suç işlenmeden suçun önüne geçebilmesine yönelik pilot uygulamaları hayata geçirmiştir[30].

Hiç şüphesiz bu uygulamalar toplum güvenliği açısından fayda sağlasa da başta hareket serbestisi, kişi hürriyeti ve kişisel veriler olmak üzere temel hak ve hürriyetler yönünden de birtakım sakıncaları beraberinde getirebilmektedir.

İngiltere'nin Romford bölgesinde polis tarafından yapılan uygulamalarda, yüz tanıma teknolojisine sahip kameraların bulunduğu alanlara giren bazı vatandaşların kameralar tarafından taranmayı reddetmeleri üzerine haklarında idari para cezası uygulanmıştır. Bu uygulama tartışma konusu olmuş ve kişilerin yüzünü örtme hakkının olup olmadığı gündeme getirilmiştir. Polis tarafından yapılan açıklamada, kişilerin bunu reddetmesinin onları bir suç şüphelisi haline getirmeyeceği dile getirilmiştir. Romford bölgesinde 8 saat süreyle yapılan uygulamada, yüz

---

29 https://www.bbc.com/turkce/haberler-dunya-44865198 (e.t.:04.10.2019)

30 http://www.milliyet.com.tr/teknoloji/ingiliz-polisi-sucu-onlemek-icin-yapay-zeka-kullanacak-2786584 (e.t.:04.10.2019); Bu gelişme sonrasında, basında, sinema tarihinin önemli filmler arasında yer alan "Azınlık Raporu" filmindeki teknolojinin gerçeğe dönüştüğü yorumları dile getirilmiştir. Bkz. http://www.hurriyet.com.tr/avrupa/azinlik-raporu-filmi-gercek-oluyor-sucu-islenmeden-onleme-donemi-basliyor-41035280 (e.t.: 04.10.2019)

tanıma teknolojisi sayesinde davranışları şüpheli görülen bir kişi durdurulmuş ve çeşitli suçlardan aranan şahıslar tespit edilerek gözaltına alınmıştır[31].

Güvenliğin sağlanması ve suçun önlenmesi adına İngiltere'nin çeşitli bölgelerinde yapılan bu uygulamalar, ülkede hem etik hem de hukuki tartışmaları beraberinde getirmiş, eleştirilere konu olmuştur. Bazı insan hakları savunucuları, yüz tanıma teknolojisinin kamusal alanlarda kullanımının, kişisel verileri ihlal ettiği, bu uygulamanın rıza dışı parmak izi alma ya da DNA analizi yapma ile eşdeğer olduğu ve kişinin haklarını ihlal ettiği yönünde eleştiriler dile getirmiştir[32].

Hiç şüphesiz, güvenliğin sağlanması ve suçun önlenmesi amacıyla geliştirilen yapay zeka uygulamalarının, yasal düzenlemeler yoluyla ve hak ve özgürlük-güvenlik arasındaki denge gözetilerek tatbik edilmesi son derece önem taşımaktadır. Bu teknolojilerin meşruiyet kazanbilmesi için, yasaya dayanması ve orantılı bir şekilde tatbik edilmesi gerekmektedir. Aksi halde, her nerede uygulanırsa uygulansın, bu ve benzeri uygulamaların etik ve hukuki meşruiyeti her zaman tartışmaya açık olacaktır.

Kamusal alanlarda suçun önlenmesi ve suç şüphelilerin tespitinin yanı sıra, bu amaca yönelik teknolojiler spesifik alanlarda da kendisini göstermektedir. Örneğin ABD'de, QuantaVerse firması, finansal suçların önüne geçebilmek, mali kurumların ve banka müşterilerinin dolandırıcılığa karşı korunmasını sağlamak amacıyla *CAE Checkup* isimli yapay zeka sistemi geliştirmiştir. Bu yazılım, verileri analiz ederek şüpheli işlemleri hızlı biçimde tespit edebilme özelliğine sahiptir[33].

Öte yandan, toplum güvenliğinin sağlanması amacıyla, bazı global firmalar suç öngörme yazılımı adı altında çeşitli yapay zeka uygulamaları geliştirdiklerini açıklamışlardır. Örneğin *Hitachi* şirketi, CCTV kameralar, toplu ulaşım haritaları, hava durumu raporları ve hatta sosyal medya yayınları gibi büyük bir veri kaynağı ağından alınan büyük miktardaki verileri hızla inceleyerek belirli bir bölgede suçların nerede işlenmesinin daha muhtemel olduğunun öngörülebildiğini duyurmuştur. Şirket bu teknolojinin en önemli özelliğinin, suçun öngörülmesiyle ilgili verilerin analizi konusunda insani önyargıların bertaraf edildiğini, makine öğrenimi teknolojisi sayesinde yalnızca veriler kullanılarak hareket edildiğini, bu öngörülerden hareketle, şehirler dahilinde sıklıkla suç işlenen noktaları gösteren ısı haritalarının oluşturulduğunu ve böylece kaynakların

---

31 https://www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met-police-face-cover-man-fined-a8756936.html (04.10.2019)

32 https://www.bbc.com/news/uk-48315979 (04.10.2019)

33 https://fintechistanbul.org/2017/12/26/finansal-suclari-engellemek-icin-yapay-zeka-devrede/ (e.t.:04.10.2019)

suça tepki vermek yerine suçu önleyecek şekilde kullanılmasının mümkün kılındığını açıklamıştır[34].

2. Ceza Muhakemesi Sürecinde Yapay Zeka Uygulamaları

Günümüz teknolojisinin ulaştığı seviye, tüm alanlarda olduğu gibi hukuk alanında da yapay zeka sistemlerinin kullanımını beraberinde getirmektedir. Hali hazırda hukuk ve adalet sistemi bakımından yapay zeka uygulamalarının başlangıç düzeyinde bir kullanım imkanı ortaya çıkardığını ifade etmek gerekir.

Yukarıda da yer verdiğimiz gibi, dünyanın çeşitli ülkelerinde ortaya çıkan ve kullanımına başlanan yapay zeka yazılımları incelendiğinde, bu uygulamaların doğal dil işleme tekniğiyle hukuki sahada önemli görevler ifa etmeye başladığı söylenmelidir.

Her ne kadar yapay zeka sistemlerinin kullanımı ve getirdiği kolaylıklar henüz, tıp, tarım, sanayi, güvenlik gibi alanlardan farklı olarak hukuk uygulamaları bakımından olmazsa olmaz bir düzeye erişmemişse de, yakın gelecekte diğer alanlarda olduğu gibi hukuk uygulamasında da vazgeçilmez bir yer edinebileceğini öngörmek hiç de zor değildir.

Hiç şüphesiz, hukuk uygulamalarının önemli bir boyutunu ceza muhakemesi süreçleri oluşturmaktadır. Ceza muhakemesi, suç şüphesinin ortaya çıkmasından başlayıp, yargı makamlarınca verilen hükmün kesinleşmesine kadar geçen süreci ifade etmektedir.

Ceza muhakemesi, ceza hükmü içeren kurallara aykırı hareket edilip edilmediğinin araştırıldığı, iddia, savunma, yargılama makamlarının bir dizi faaliyetinden oluşan ve usul hukuku kurallarına uygun şekilde yürütülecek adil bir muhakeme neticesinde maddi gerçeğe ulaşmayı hedefleyen sürece verilen addır[35].

---

[34] https://www.hitachi.eu/tr-tr/sosyal-inovasyon-hikayeleri/teknoloji/teknoloji-suca-karsi-savasta-gizli-silahimiz (e.t.:04.10.2019)

[35] Beulke, Werner, Strafprozessrecht, 11. Auflage, Heidelberg 2010, s.4,5, kn.8; Roxin C., Schünemann B., Strafverfahrensrecht, 27. Auflage, München 2012, s.1, kn.1; Volk K., Grundkurs StPO, 7. Auflage, München 2010, s.2,3, kn.1,2; Schmid N., Strafprozessrecht, Zürich 1989, s.1,2, kn.2,3; Krey V., Deutsches Strafverfahrensrecht, Band 1, Stuttgart 2006, s.1, kn.2; Ostendorf H., Strafprozessrecht, 1. Auflage, Baden-Baden 2012,s.26, 27, kn.1,2; Soyaslan D., Ceza Muhakemesi Hukuku, 5. Baskı, Ankara 2014, s.53; Öztürk B. vd., Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, 12. Baskı, Ankara 2018, s.27, 28; Centel N., Hamide Z., Ceza Muhakemesi Hukuku, Ankara 2014, s.3; Ünver Y., Hakeri H., Ceza Muhakemesi Hukuku, 10. Baskı, Ankara 2015, s.1; Gökcen A., Balcı M., Alşahin M. E., Çakır K., Ceza Muhakemesi Hukuku, Ankara 2018, s.29; Yenidünya C., İçer Z., Ceza Muhakemesi Hukuku, Ankara 2016, s.1, 2; Şahin C., Ceza Muhakemesi Hukuku I, 9. Bası, Ankara 2018, s.27; Yenisey F., Nuhoğlu A., Ceza Muhakemesi Hukuku, 6. Baskı, Ankara 2018, s.67, 68; Özbek V. Ö., Doğan K., Bacaksız P., Tepe İ., Ceza Muhakemesi Hukuku, 11. Baskı, Ankara 2018, s.37.

Ceza muhakemesi, soruşturma ve kovuşturma olmak üzere iki temel evreden oluşur. Suç şüphesinin ortaya çıkmasından iddianamenin kabulüne kadar geçen evre soruşturmayı, iddianamenin kabulünden hükmün kesinleşmesine kadar geçen evre ise kovuşturmayı ifade etmektedir (CMK m.2).

Soruşturma ve kovuşturma evreleri, bütün olarak ceza muhakemesi sürecini meydana getirir. Ceza muhakemesi, iddia, savunma ve yargılama olmak üzere üç temel faaliyetten oluşur. Cumhuriyet savcısı, kamu adına iddia faaliyetini yerine getirirken, mağdur, suçtan zarar gören, katılan ve vekilleri iddia faaliyetine bireysel olarak katkı sağlar.

Savunma tarafında ise, suç isnadı altında bulunan şüpheli, sanık ve kamusal savunma makamı olarak müdafi yer almaktadır. Soruşturma evresinde şüpheli, kovuşturma evresinde sanık, ister bireysel olarak isterse müdafi yardımından yararlanmak suretiyle, kendisine yöneltilen suç isnadını ortadan kaldırmaya çalışır.

İddia ve savunmanın ortaya koyduğu tez ve antitezden bir sonuç çıkartarak, ceza uyuşmazlığını çözüme kavuşturan yargılama merci ise, bağımsız ve tarafsız olarak görevini yerine getiren mahkemelerdir.

İddia, savunma ve yargılamadan oluşan ceza muhakemesi faaliyeti, kompleks yapıdaki bir süreci ifade etmektedir. Bu süreçte, ceza muhakemesi faaliyetini yürüten süjelerin, sözlü, yazılı, eylemsel ve elektronik olmak üzere dört kategori altında işlemlerde bulunabilme imkanına sahiptir[36]. Son yıllarda, ülkemizde yargısal süreçlere dahil olan UYAP, SEGBİS gibi sistemler aracılığıyla elektronik birtakım işlemler de yapılabilir hale gelmiştir. Bu teknik yöntemlerin kullanılması, birtakım işlemlerin yapılmasını hızlandırmakta ve bu durum usul ekonomisine hizmet etmektedir.

Teknolojik gelişime ve yapay zeka sistemlerinin ulaştığı seviyeye göre, dönemsel olarak, yukarıda sözünü ettiğimiz bu akıllı sistemlerin sürece katkısının değişkenlik gösterebileceğini ifade etmek gerekir. Bu dönemler, kısa (5-15 yıllık süreç), orta (15-30 yıllık süreç), uzun (30 yıl ve sonraki dönem) vade olmak üzere üç şekilde sınıflandırılabilir.

Yapay zeka uygulamalarının geleceği açısından öngörülerde bulunurken, bu dönemlerin, ceza muhakemesi faaliyetleri bakımından ayrı ayrı değerlendirme konusu yapılmasında fayda bulunmaktadır.

---

36 Ünver-Hakeri, s.121; Yenisey-Nuhoğlu, s.111-117; Yenidünya-İçer, s.214-217; Öztürk vd., s.281, 282.

2. İddia Faaliyeti Açısından

İddia faaliyeti, yargı organizasyonu içerisinde savcılıklar aracılığıyla yerine getirilmektedir. Savcılığın bu faaliyeti yerine getirdiği sırada en önemli yardımcısı kolluk güçleridir. Adli kolluk hizmetleri, savcılık tarafından alınan kararların hayata geçirilmesinde önemli rol oynar. Soruşturma işlemlerinin yerine getirilmesi ve koruma tedbirlerinin uygulanmasında adli kolluk personeli, savcı tarafından verilen emir ve talimatlar doğrultusunda hareket eder (CMK m.161/2).

Bazı ülkelerde emniyet birimleri, suçun önlenmesi ve güvenliğin sağlanması amaçlarının (idari kolluk faaliyeti) dışında, adli kolluk faaliyetleri açısından da yapay zeka teknolojisinden yararlanmaya yönelik çalışmalara hız vermiştir. Örneğin İngiltere'de Durham emniyeti, tutuklanan bir şüphelinin toplum için arz ettiği olası tehdidi değerlendirmek ve gözaltında tutmaya veya kefaletle serbest bırakmaya karar vermek için *"Zarar Değerlendirme Riski"* aracı adı verilen bir yapay zeka yazılımını test etmiştir. Sistem algoritması, 2008-2012 arasında toplanan verileri ve şüphelinin cinsiyeti ile posta kodunu kullanarak karar verecek şekilde oluşturulmuştur. İki sene boyunca test edilen yazılım bir şüphelinin düşük risk arz ettiğini %98 oranında öngörmeyi başarmıştır. Sistemin en az hataya sebebiyet vermek adına temkinli bir şekilde oluşturulduğu ve özellikle ilk aşamada tehlikeli olabilecek şüphelilerin serbest bırakılmasını önlemek amacıyla programlandığı ifade edilmiştir[37].

Adli kolluk hizmetleri kapsamında, suç işlendikten sonraki çalışmalara yönelik yapay zeka uygulamalarının önemli bir rol üsteleneceğini belirtmek gerekir. Dünyada hali hazırda bu amaçla test edilen yazılımlar bulunmaktadır. Henüz başlangıç seviyesinde olsa da yakın gelecekte yapay zeka kullanımının adli kolluk faaliyeti açısından son derece önemli kolaylıklar getireceğinde tereddüt bulunmamaktadır. Örneğin Birleşik Krallık'taki West Midlands Polis teşkilatı, fiziksel olarak temizlendikten çok sonra olay yerini sanal olarak incelemeye olanak tanıyan bir teknolojinin kullanımına öncülük etmektedir. Bu uygulama kapsamında, olay yerinin incelenmesi bakımından, olay yerinin uzaktan doğru şekilde haritalanmasını sağlayan 3D lazer tarayıcılar geliştirilmiştir. 3D lazer teknolojisi, saniyede on binlerce noktalık bir hızla, olay yerinin boyutlarını ölçebilmekte ve bu verilerden hareketle olay yerinin üç boyutlu bir modelini oluşturabilmektedir. Tarayıcılar tarafından yakalanan dijital fotoğraflardaki renklerle, olay yerinin modellemesi, gerçekçi bir boyuta taşınmaktadır. Böylelikle, adli kolluk güçleri, olay yerini

---

37 https://www.hitachi.eu/tr-tr/sosyal-inovasyon-hikayeleri/teknoloji/teknoloji-suca-karsi-savasta-gizli-silahimiz (e.t.. 04.10.2019)

fiziksel olarak ziyaret etmeden, olayın iz ve delilleri ortadan kaldırıldıktan sonra bile ihtiyaç duydukları kadar olay yerini inceleme fırsatı yakalamaktadır[38].

Bu teknolojilerin yanı sıra, hali hazırda ihtiyari olarak kullanılmaya başlanan doğal dil işleme sistemlerinin kısa vadede, iddia faaliyeti bakımından zorunlu hale getirilmesi ihtimal dahilindedir. Zira bu sistemlerin temel özelliği ve amacı, sürecin ve karar mekanizmalarının hızlı ve etkili bir şekilde işletilmesinden ibarettir. Ceza muhakemesinin amacı da, makul sürede ve adil bir şekilde yapılacak yargılama neticesinde maddi gerçeği ortaya çıkarmak ve böylelikle bozulan hukuk barışını yeniden tesis etmektir. Bu noktada "yargıda hedef süre" gibi amaçlar bakımından DDİ teknolojisinin biçilmiş kaftan niteliğinde olduğunu söylemek mümkündür.

Ceza muhakemesinde, tahmin teknolojisi ve belge otomasyonu altında sınıflandırılabilecek, asistan hizmeti veren yazılımların iddia faaliyetinin işlevselliğini ve başarısını artırabilecek yazılımlar olacağı şüphesizdir. Sözünü ettiğimiz yazılımların kullanım alanları değerlendirildiğinde, bu yazılımların ekseriyetle özel hukuk alanında avukatların iş ve işlemlerini kolaylaştırma amacına özgülendiği görülmekte ise de, ceza yargılamasının hazırlayıcısı konumunda olan iddia makamları yönünden bu yazılımların, son derece önemli bir işlevi yerine getirebilecek mahiyette olduğu açıktır.

Ceza yargılaması, iddia faaliyeti ile başladığından ve sürecin başarısı iddia faaliyetinin etkinliği ile doğru orantılı olduğundan, hem tahmin teknolojisi hem de belge otomasyon sistemlerinin kullanımı, savcılık müessesinin etkinliğini artıracak, bu durum ceza yargılamasının amaçlarına ulaşmasında önemli bir rol oynayabilecektir.

İddiasız savunma olamayacağı gibi, davasız yargılamanın da olmayacağı, ceza muhakemesi hukukunun temel prensiplerinden biridir (davasız yargılama olmaz ilkesi)[39]. Bu sebeple, ceza adalet sisteminin suçlu ile suçsuzu ayırt edebilecek hızlı ve etkili bir hazırlık mekanizmasını oluşturması, gereksiz dava açılmasının önüne geçecek, dava açıldığında da makul sürede yargılamanın sonlandırılmasına katkı sağlayacaktır.

Bu açıdan, ceza muhakemesinde, suç şüphesinin ortaya çıkmasından, hükmün kesinleşmesine kadar, işlendiği iddia edilen bir suçun ortaya koyduğu şüphe giderilmeye ve ortadan kaldırılmaya çalışılmaktadır. Soruşturma evresi, şüphenin mutlak bir şekilde ortadan kaldırılmasının gerekli olmadığı, yalnızca şüphenin olgunlaşması ve yeterli şüphe düzeyi (CMK m.170, 171) ile

---

38 https://www.hitachi.eu/tr-tr/sosyal-inovasyon-hikayeleri/teknoloji/teknoloji-suca-karsi-savasta-gizli-silahimiz (e.t.. 04.10.2019)

39 Öztürk vd., s.145; Ünver-Hakeri, s.46; Yenisey-Nuhoğlu, s.75; Özbek-Doğan, Bacaksız-Tepe, s.70.

yetinilebilecek bir evre olarak karşımıza çıkmaktadır. Şu halde, soruşturma evresinin, yargısal bir hükmün verilmediği, maddi gerçeğin araştırılarak, yargısal sürece hazırlık oluşturan birtakım işlemlerin yapıldığı bir evre olduğunu söylemek mümkündür.

Kişinin mahkum olma ihtimalinin, beraat etme ihtimalinden fazla olduğu (yeterli şüphenin bulunduğu) kanaatine Cumhuriyet savcısı tarafından ulaşılmasıyla birlikte, savcının iddianame denilen yazılı bir belge ile süreci yargılama aşamasına taşıması, soruşturma evresini sona erdiren yazılı bir işlem niteliğindedir.

Tahmin teknolojisi kategorisinde değerlendirilebilecek olan yazılımların, büyük ölçüde dava sonuçlarını tahmin edebildiği yönündeki tespitler dikkate alındığında, bu nitelikteki yazılımların, soruşturma evresinde iddia makamlarının yararlanabileceği önemli yazılımlardan olabileceğini ifade etmek gerekir.

Nitekim ceza yargılaması uygulamasında en önemli sorunlardan biri olan, açılan davalardaki mahkumiyet – beraat kararları arasındaki orantısal dengesizlikler, soruşturma evresinin etkin ve doğru bir şekilde işletilememesi, bu tip sistemlerin kullanım ihtiyacını artıracak unsurlardır. Nitekim tüm dünyada ve ülkemizde yargı ve ceza adaleti stratejileri, iddia faaliyetinin kuvvetlendirilmesini, gereksiz davaların açılmasının önüne geçilmesini, yargının iş yükünün ve dava süreçlerinin azaltılmasını, yargı dışı alternatif yöntemlerin genişletilmesini öngörmektedir.

Bilhassa ülkemizde son dönemlerdeki getirilen yasal düzenlemelerle Cumhuriyet savcılarının takdir yetkilerinin artırılması, uzlaştırmanın kapsamının genişletilmesi, seri ve basit yargılama usullerinin belirlenmesi, aynı amaca hizmet eden uygulamalar olarak değerlendirilmelidir. Bu gelişmeleri tamamlayıcı olarak, tahmin teknolojisinin iddia faaliyeti açısından kullanımının zorunlu hale getirilmesi, kısa ve orta vadede yargı ve ceza adaleti stratejisi açısından üzerinde ciddiyetle durulabilecek uygulamalardan biri olabilir. Böylelikle devlet adına iddia faaliyetini yürüten savcılık müessesesi, tüm yargılama sürecini etkileyen ve davanın temelini oluşturan iddia faaliyetini daha başarılı ve etkili bir şekilde yerine getirmiş olacak, aynı zamanda ceza uyuşmazlıklarının alternatif yöntemlerle ya da seri, basit yargı usulleri ile çözümünde bu uygulamaların kullanılması, bu müesseselerden beklenen faydanın daha kolay bir şekilde elde edilebilmesine olanak tanımış olacaktır.

Genel soruşturma usulüne göre, Cumhuriyet savcısı, adli kolluk marifetiyle soruşturma evresinde, şüphelinin lehinde ve aleyhinde olan delilleri toplayarak, işin gerçeğini araştırmaya başlamakla görevlidir (CMK m.160). Gerektiğinde sulh ceza hakimine müracaat ederek, hakim kararı

gerektiren belirli koruma tedbirlerinin (tutuklama, teknik araçlarla izleme, iletişimin denetlenmesi gibi) uygulanmasını talep edebilir. Bu tedbirlerin uygulanması belirli şartlara tabidir.

Soruşturma işlemleri açısından belirli bir silsile olmadığı gibi, bu işlemler zaman ve mekandan bağımsız olarak yapılmaktadır. Bu işlemlerin sırası ve türü, somut olayın özelliklerine, Cumhuriyet savcısının bilgi, birikim ve tecrübesine bağlı olarak değişkenlik gösterebilmektedir. Bu durum, soruşturma evresinin dağınık olduğunu ve belirli bir kurala bağlı olmadığını ortaya koyan özelliklerdir[40].

Kuşkusuz, kısa ve orta vadede olması muhtemel gözüken bu gelişmeler, uzun vadede iddia faaliyetinin bir insandan arındırılarak yerine getirilebileceği şeklinde bir yoruma mahal vermemelidir.

Doğal dil işleme tekniği kullanılarak, söz konusu yazılımların iddia faaliyetini yürüten makamlara yardımcı olabilmesi mümkün ise de, iddia faaliyeti yalnızca araştırma ve soruşturma işlemlerinin yapılması, delillerin toplanması gibi eylemsel (fiili, fiziki) işlemlerden ibaret olmayıp, iddianame düzenlenmesi, kovuşturmaya yer olmadığına ilişkin karar verilmesi, kamu davasının açılmasında takdir yetkisinin kullanılması, seri yargılama usulü çerçevesinde ceza tayin edilmesi gibi hukuki yorum, değerlendirme ve sübjektif karar alma süreçlerine ihtiyaç duyulan karar mekanizmalarını da içerisinde barındırmaktadır. Bu meyanda, Cumhuriyet savcısının soruşturma evresinde, son derece kompleks yapıda görev tanımları bulunduğundan, bu görevlerin münhasıran yapay zeka sistemleri tarafından yerine getirilebilmesi yakın ve uzak gelecekte pek mümkün gözükmemektedir.

Günümüz teknolojisinde genel yapay zekanın gelişmişlik seviyesi henüz hukuki yorum, muhakemede bulunma gibi bilişsel faaliyetleri gerçekleştirme düzeyine ulaşmadığından, kısa ve orta vadede iddia faaliyetinin mutlaka bir insan kontrolünde icra edilmeye ve sonuçlandırılmaya devam edeceği ve etmesi gerektiği kanaatindeyiz.

3. Savunma Faaliyeti Açısından

Savunma faaliyeti, ceza muhakemesinin üç faaliyetinden biridir. Şüpheli, sanık ve müdafi tarafından yürütülen bu faaliyet, iddianın geçersizliğini, yanlışlığını, eksikliğini ortaya koymakta ve bu suretle yargılama makamı tarafından verilecek hükme tesir etmeye çalışmaktadır.

---

40 Yenisey-Nuhoğlu, s.551; Ünver-Hakeri, s.520, 521; Yenidünya-İçer, s.245.

Avukatlık görevinin etkin ve zamanında yerine getirilmesi amacıyla oluşturulan programlar ile tahmin teknoloji ve hukuki analitik adı altında sınıflandırılan yazılımların, avukatlık mesleğine önemli katkılar sağlayacağında tereddüt bulunmamaktadır.

Günümüzde de örneklerine rastladığımız, avukatların görevlerini yerine getirmesine yardımcı olan programlar, özellikle avukatların duruşma günlerini not edebilmesi, randevuların oluşturulabilmesi, dava türlerinin tasnifinin ve sistemdeki kaydının yapılabilmesi, dava dilekçelerinin hazırlanması, yasa değişikliklerinin ve güncel yargı içtihatlarının takip edilmesi bakımından büyük kolaylıklar getirmektedir. Ülkemizde Kazancı, Sinerji gibi programlar, buna örnek gösterilebilir.

Tahmin teknolojisi adı altında kategorize edilen sistemler, benzer uyuşmazlıklardaki yargı içtihatlarının tespit edilmesinin yanı sıra, çeşitli bilgileri bu programlardaki sistemlere işlemek suretiyle, uyuşmazlığın muhtemel sonuçları hakkında hızlı ve kolay bir şekilde bilgi sahibi olunabilmesi gibi işlevleri yerine getirecektir. Elbette, bunun programı kullanan kişiler bakımından pratik sonuçları söz konusu olacaktır.

Ülkemizde Kodex Bilişim tarafından geliştirilen *ARYA* isimli yazılımın, Yargıtay'daki davaların sonuçlarını %90 oranında doğru tahmin edebildiği ifade edilmektedir[41]. *Hukuk Work* isimli yazılım ise, mevcut bir uyuşmazlığın ne şekilde sonuçlanacağını en güncel mevzuat, içtihat değişiklikleri ve son yargı kararları ışığında ortaya koyabilen bir algoritmaya sahiptir[42]. Bunun gibi, *Turklex* programı, hukukçuların tüm ihtiyaçlarını karşılamayı amaçlayan yapay zekâ ürünü yeni nesil bir yazılım olup, en güncel mevzuatlara, yargı kararlarına ulaşma imkanını sunmasının yanı sıra, dava dosyasının otomatik şekilde oluşturulması, davanın sonuçlanma olasılığını analizlerle öngörebilmesi (dava sonuç analizi) gibi önemli işlemleri yerine getirebilmektedir[43].

Bilhassa avukatlar tarafından bu tarz programların kullanılması, onların yapacakları hukuki destek ve hukuki yardımlar açısından büyük kolaylıkları beraberinde getirebilecektir. Avukatlar bu sayede, müvekkillerine ya da hukuki danışmanlıkta bulundukları kimselere daha hızlı ve kolay bir şekilde bilgi aktarabilecek ve uyuşmazlığın çözümü noktasında kendilerinden beklenen katkıları sağlayabilecektir. Dava sonuç analizine de olanak tanıyan bu uygulamalar, özellikle dava stratejilerinin belirlenmesinde önemli bir rol oynayacaktır.

---

41 https://www.webtekno.com/turkiye-deki-yargitay-davalarini-dogru-tahmin-eden-yapay-zeka-gelistirildi-h58904.html (e.t.: 30.09.2019)

42 https://www.hukukmedeniyeti.org/haber/20192/hukuk-bilgi-sistemi-hukuk-work-yay-n-hayat-na-ba-l/ (e.t.:30.09.2019)

43 https://www.turklex.com/hukuki-analiz/ (e.t.: 30.09.2019)

Hukuki analitik yazılımları ise, tahmin teknolojisinden daha ileri düzeyde bir işleve sahiptir. Bu yazılımlar, yalnızca uyuşmazlığa ilişkin özellikleri değil, sürece etki eden uyuşmazlık içi ya da dışı tüm faktörleri değerlendirerek, sürece ilişkin adeta bir simülasyon gerçekleştirmektedir. Hukuki analitik yazılımlarının, savunma faaliyeti açısından son derece önemli görevler ifa edeceği açıktır.

Sözünü ettiğimiz bu programların giderek yaygınlaşacağını ifade etmek mümkündür. Bununla birlikte, bu tarz programların kimler tarafından kullanılmasının yerinde olacağı tartışmaya açılmalıdır. Nitekim bazı gelecek bilimcileri, YZ'nin yakın gelecekte pek çok insanı işinden edeceği yönünde öngörülerde bulunmakta ve hukuki sahada avukatlar, gelecekte mesleklerinin yapay zekalı sistemler tarafından yerine getireceği endişesini taşımaktadır.

Düşüncemize göre, avukatlık mesleği, hukuki uyuşmazlıklar var olduğu müddetçe varlığını devam ettirecektir ve ettirmelidir. Hukuki yardımın niteliği, hukuki destek ve süreçlerde stratejilerin belirlenmesi, uyuşmazlığın çözümü noktasında yorumsal faaliyet ve muhakeme yeteneği, insana özgü özelliklerdir.
Bu anlamda, avukatlar tarafından sağlanan hukuki destek ve onların sistem içerinde yerine getirdikleri görevler, münhasıran hukuk bilgisi ve tecrübesine sahip kimseler tarafından yerine getirilebilecektir.

Öte yandan, adalet sisteminin işleyişinde, insana dair psikolojik faktörler de bulunmakta olup, adalet psikolojisinden soyutlanmış bir sistemden ve savunma faaliyetinin mevcudiyetinden söz etme imkanı bulunmamaktadır. Zira, YZ sistemleri, henüz insan zekası ile eşdeğer bir düzeye erişmemiştir. YZ sistemlerinin, yorum, muhakeme, risk alma, tahminde bulunma gibi bilişsel özellikleri yerine getirilebileceği veya duygulanma, hayal etme, içgüdüsel olarak davranma gibi yalnızca insana ait nitelik ve becerilere sahip olup olmayacağı konusunda henüz bilimsel bir kesinlik mevcut değildir.

Bununla birlikte, sözü edilen bu program ve yazılımlara erişim ve kullanma yetkisinin münhasıran avukatlara bırakılmayıp, genele yayılması ve herkesin programlardan istifade imkanının sağlanması durumunda, bireyler, hukuki yardım almak için avukatlara müracaat etmeye ihtiyaç duymayacaktır. Bu durum, avukatlar bakımından ciddi bir iş ve ekonomik kayıp anlamına geleceğinden, mesleğin geleceği açısından mahsurlu bir tablo ortaya çıkarabilecektir.

Kanımızca, böyle bir çıkmaza düşülmemesi adına, adalet sisteminin, bu tarz programların kullanım yetkisinin sınırlandırılması başta olmak üzere, avukatlık mesleğini koruyucu ve

destekleyici önlemleri etkin bir şekilde ve zamanında alması, teknolojik gelişmelerin meslek bakımından getirdiği dezavantajların önüne geçebilecektir.

4. Yargılama Faaliyeti Açısından

Yargılama faaliyeti, ceza muhakemesinin üç faaliyetinden biridir. İddia ve savunmanın ortaya koyduğu tez ve antitezden bir sonuç çıkarmak ve ceza uyuşmazlığını çözerek bir hükme varmak şeklindeki faaliyetlerden oluşmakta olup bu faaliyet millet adına bağımsız mahkemelerce yerine getirilmektedir. Hakim, bağımsız ve tarafsız bir kişi olarak, yargılama makamında yer alan gerçek bir kişidir.

Ceza muhakemesinde resen araştırma ilkesi geçerli olup, yargılama faaliyetini yürüten mahkeme, iddia ve savunmanın getirdiği delillerle yetinmek zorunda değildir, kendisi de delil araştırabilir[44].

Bunun sonucu olarak, ceza yargılamasının benimsediği delil sistemi, medeni yargılamadan farklılık göstermektedir. Medeni yargılamada belirli uyuşmazlıklarda belirli deliller ispata konu oluşturabilirken, ceza yargılamasında "hukuka uygun elde edilmiş olmak kaydıyla" her şey delil olabilmekte ve hakim vicdani kanaatine göre bu delilleri takdir edebilmektedir. Bu özellik, ceza muhakemesi hukukunda *"delillerin serbestliği ilkesi ve vicdani delil sistemi"* ile açıklanmaktadır[45].

Hangi delilin, o uyuşmazlığın çözümü bakımından etkili olduğu, diğer bir ifadeyle delilin ispat değerinin ne olduğu, derecelendirilebilir, kesin bir ölçüye sahip değildir. Bu sebeple, ispat faaliyeti, ceza muhakemesi sürecinin en zor faaliyetlerinden biri olup, yargılama faaliyetinin en önemli parçasını oluşturmaktadır.

İspat faaliyetini, hüküm verme faaliyeti takip eder. Hakim, huzuruna getirilmiş ve duruşmada tartışılmış delilleri değerlendirerek vicdani kanaatine göre uyuşmazlık ile ilgili bir neticeye vararak hüküm tesis eder. Hüküm, hakimin vicdanında, o aşamaya kadar var olan şüphenin yenildiği, belliliğe (sübuta) ulaşıldığı anlamına gelir.

Kısacası, ispat ve hüküm verme faaliyeti, bütünüyle hukuki bir değerlendirme ve muhakeme sürecinden oluşmaktadır. Hiç şüphesiz YZ sistemler, ispat faaliyeti sırasında hakime yardımcı

---

44 Ünver-Hakeri, s.63; Yenisey-Nuhoğlu, s.488.

45 Şahin C., Göktürk N., Ceza Muhakemesi Hukuku II, 7. Bası, Ankara 2018, s.27; Yenidünya-İçer, s.562; Ünver-Hakeri, s.65; Öztürk vd., s.152; Yenisey-Nuhoğlu, s.750 vd.

olabilecek birtakım işlevleri yerine getirebilecektir. Belirli bir delilin toplanması, delillerin yorumlanması, sanığın geçmişi ve suç işleme potansiyelinin değerlendirilmesi ve böylelikle cezanın tespiti ve bireyselleştirilmesi gibi işlem ve kararlarda, YZ sistemleri, yargı makamlarına yardımcı olabilecek ve böylelikle yargılama faaliyetine son derece önemli katkılar sağlayabilecektir. Hiç kuşkusuz YZ sistemlerinin karar mekanizmalarının oluşturulmasında kullanımının yaygınlaşması, yargısal süreçleri hızlandıracak, yargı makamlarının işini oldukça kolaylaştıracaktır.

YZ sistemlerinin, ispat faaliyetine açısından yapabileceği katkı, bilirkişilik müessesesiyle mukayese edilebilir. Bilirkişinin kendisi ya da ortaya koyduğu görüş, bir delil olmayıp, delillerin değerlendirilmesinde araçtır. Bunun gibi, delillerin yorumu ve değerlendirilmesinde YZ yazılımları oldukça işlevsel bir görev ifa edebilecektir. Bunun gibi, tercümanlık hizmetlerinde YZ yazılımları önümüzdeki yıllarda, insanın yerini alabilecek ve insana ihtiyaç duyulmaksızın bu hizmetler yerine getirilebilecektir. YZ sistemlerinin, belirli bir işlemi insan gibi yapabilme kapasitesine ilişkin yapılan öngörülerde, dil tercüme etme açısından 2024 yılına işaret edilmektedir[46].

Hukuki analitik ya da tahmin teknolojisinin, yargılama faaliyeti açısından yararlı olabilecek teknolojiler olduğu ifade edilebilirse de, söz konusu yazılımların günümüz teknolojisiyle tek başına yargılama faaliyetini yerine getirebilecek bir düzeyde olduğunu söyleme imkanı yoktur.

İspatın nisbiliği, delillerin serbestçe değerlendirilmesi, vicdani delil sistemi, kararların gerekçeli olması gibi ceza yargılamasına ilişkin özellikler, karar verici olarak bir insanın (hakimin) varlığını zorunlu kılmaktadır. Nitekim, vicdani kanaat edinme, yorumlama ve bu doğrultuda hükme varabilme, insana özgü özellik ve becerilerdir. Doğuştan ve yaradılış gereği içgüdüsel olarak duygu ve düşünme yeteneği olmayan, vicdanına göre karar veremeyen YZ sistemlerinin, bir insan gibi yargılama faaliyetini yerine getirebilmesi imkan dahilinde değildir.

Bu noktada akıllı teknolojilerle donatılmış yapay zeka sistemli hakimleri yargılamada kullanmaya başlayan Çin Halk Cumhuriyeti, incelemeye şayan bir örnektir. Zira Çin, etik tartışmalara sebebiyet verecek alanlarda bu hakimlerin kullanılmaması gerektiğini öngörmek suretiyle teknolojinin getirdiği yenilikleri yargılama sahasına taşırken oldukça mutedil davranmıştır. Bu temkinli yaklaşım doğrultusunda Çin'de yapay zeka ürünü hakimlerin yargılama evresindeki rolü,

[46]https://twitter.com/valaafshar/status/934143443886133250?ref_src=twcamp%5Eshare%7Ctwsrc%5Eios%7Ctwgr%5Enet.whatsapp.WhatsApp.ShareExtension%7Ctwcon%5E7100%7Ctwterm%5E0 (e.t.:04.10.2019)

yalnızca tekrarlayan işlerin tamamlanmasında yargılamanın esas süjelerine yardımcı olmakla sınırlandırılmıştır[47].

Kanaatimizce teknolojinin geldiği nokta temel alındığında bu, oldukça faydalı bir yaklaşımdır. Zira bu yaklaşım; bir yönüyle yargılama çağın şartlarına adapte edilerek uyuşmazlıkların çözümünde insan emeğinin kapasitesiyle ulaşılması mümkün olmayan bir hıza erişmeyi içerirken, diğer taraftan toplumda henüz ortak kabule konu olmamış yapay sistemlere karşı doğabilecek olası etik tepkilere karşı temkinli bir politikayı ihtiva etmektedir.

Günümüz yapay zeka teknolojisi ele alındığında yapay hakimlerin, medeni usul hukukunun sınırlı delil ilkesi gereğince örneğin ticaret ve icra mahkemelerinde görülen davalarda mükerrer işleri yapmakta oldukça başarılı olacaklarına şüphe yokken, ceza muhakemesi hukuku özelinde aynı sözleri sarf etmek mümkün değildir. Zira ceza yargılaması, vicdani delil sistemine dayanmaktadır. Her ne kadar doğal bir vicdana yaklaşacak ve hatta geçecek kadar geniş bir veri tabanıyla besleniyor olursa olsun, henüz bir bilince sahip olmadıklarından yapay zeka sistemlerinin vicdani delil sisteminin gerektirdiği şartları sağlamadığı, hülasa mevcut hâliyle ceza yargılaması için uygun olmadığı ifade edilmelidir.

Keza, verilen bir karar ya da hükmün gerekçesinin gösterilmesi de, ceza yargılamasının vazgeçilmez unsurlarından biridir. Belirli bir sonuca hangi sebeple ulaşıldığının ortaya konulması, yargılamanın şeffaf ve adil olması açısından olmazsa olmaz bir gerekliliktir. Bu gereklilik, aynı zamanda açıklanabilirlik ve hesap verebilirlik ile de yakından ilgilidir. Gerekçe gösterme zorunluluğu, keyfiliği ortadan kaldırdığı gibi hukuki denetime olanak veren bir özelliğe sahiptir.

YZ sistemleri, programlanan algoritmaların, insan beynindeki nöral ağların taklit edildiği yapay sinir ağlarının etkileşime geçmesiyle birlikte, belirli bir yönde karar alabilmektedir. Fakat, insan davranışlarında olduğu gibi yapay zekanın da belirli bir kararı nasıl ve niçin aldığı bilinmemektedir[48]. Bu açıdan YZ sistemleri sonuç odaklı sistemler olup karar verme süreçleri denetlenememektedir. YZ sistemlerinin belirli bir kararı niçin aldığının açıklanamaz olmasının, insanlar nezdinde YZ'nin aldığı kararlar açısından güvenilirlik sorununu ortaya çıkardığı ifade edilmektedir[49]. Hatta bir kısım YZ uzmanlarınca, aldıkları kararların, karar verme esaslarının,

---

47 http://www.hurriyet.com.tr/teknoloji/cinde-mahkemelerde-yapay-zeka-yargic-donemi-41257582 (e.t.: 01.10.2019)

48 https://t24.com.tr/haber/yapay-zeka-yarin-obur-gun-nasil-davranacak-bilemiyoruz,589739 (e.t.: 04.10.2019)

49 https://www.forbes.com/sites/jasonbloomberg/2018/09/16/dont-trust-artificial-intelligence-time-to-open-the-ai-black-box/ (e.t.:04.10.2019)

hareketlerinin denetimi ve kontrolü için YZ sistemlerinin etik bir kara kutuya (black box) sahip olması yönünde öneriler dile getirilmiştir[50].

Hali hazırda YZ sistemlerinin karar alma süreçlerindeki belirsizlik ve bilinmezlik, bu sistemlerin adalet mekanizması içerisindeki güvenilirliği açısından şüphe doğurmaktadır. YZ sistemlerinin yargısal süreçlerde ve adalet sistemi içerisindeki gelecekte ne gibi roller üsteleneceği sorunsalında, bu konuda yaşanacak gelişmeler belirleyici olacaktır.

Sonuç olarak, ceza muhakemesinde yargılama faaliyeti bir bütün olarak değerlendirildiğinde münhasıran insan tarafından yerine getirilebilecek bir faaliyettir. YZ sistemlerinin, delillerin toplanması, tasnifi ve değerlendirilmesi gibi mükerrer işlerde, hakimin yardımcısı olma noktasında oldukça verimli araçlar olacağı açıktır.

Bilhassa, delillerin değerlendirilmesi, yorumlanması, tercümanlık ve bilirkişilik faaliyetlerinin yerine getirilmesi, sanığın geçmişi ve ileride suç işleme potansiyelinin değerlendirilmesi suretiyle cezanın tespiti ve bireyselleştirilmesi gibi konularda yargılama makamlarına yardımcı olarak ispat ve hüküm verme faaliyetlerine önemli katkılar sağlayacağında tereddüt bulunmamaktadır.

Bununla birlikte, ceza yargılaması faaliyetinin tümüyle YZ sistemlerine terk edildiği bir adalet mekanizmasının düşünülmesi teknolojik açıdan gerçekçi olmadığı gibi -ceza muhakemesinin yüzyıllardır kabul ettiği ilke, prensip ve kaideler manzumesi nazara alındığında- kabul edilebilir gözükmemektedir. İnsan tarafından yerine getirilecek bir faaliyet olarak şekillendirilen ve yargılamaya ilişkin birtakım temel prensiplere göre dizayn edilen bu sistemde, vicdanına göre karar alamayan, yorumlama, muhakeme etme, aldığı kararı gerekçelendirme gibi insana özgü kabiliyetleri bulunmayan YZ sistemlerinin bir insan gibi yargılama faaliyetini yerine getirebilmesi mümkün değildir.

Son olarak ifade edelim ki, şu an için bilim-kurgudan öteye geçmese de, gelecekte kişilerin arzu, düşünce ve düş dünyaları dahil tüm iç dünyalarına bir mikroçip veya benzeri cihazlarla her an kamu gücü kullanılarak ulaşılabilecek teknolojiler üretilip yaygınlık kazandığında[51], ceza muhakemesi ve özellikle ispatla alakalı mevcut tüm regülasyon ve ilkelerin, artık "geleneksel" hâle geleceği ve hem hukuki hem içtimai bakımdan devrim niteliğinde yeni bir ceza muhakemesi sisteminin inşa edilmesinin zorunlu hale geleceği her türlü izahtan varestedir.

---

50 http://www.dijitalhabitat.com/robotlarin-denetimi-icin-kara-kutu-onerisi/(e.t.: 04.10.2019)

51 https://medium.com/@nfo94/black-mirror-subjectivity-and-technology-in-the-entire-history-of-you-e775bfd4640f (e.t.:01.10.2019); https://www.mirror.co.uk/tv/tv-news/blackmirror-thirdepisode-theentirehistoryofyou-12260563 (01.10.2019)

KAYNAKÇA

Akil C., "Türkiye Barolar Birliği Disiplin Kurulu Kararları Işığında Avukatın Görevini Özenle Yerine Getirme Yükümlülüğü Araştırma". *Hacettepe Hukuk Fakültesi Dergisi*, *2*(1), (2012).

Aletras, N., Tsarapatsanis, D., Preoţiuc-Pietro, D., & Lampos, V. (2016). Predicting judicial decisions of the European Court of Human Rights: A natural language processing perspective. *PeerJ Computer Science*, *2*.

Beulke, Werner, Strafprozessrecht, 11. Auflage, Heidelberg 2010.

Centel N., Zafer H., Ceza Muhakemesi Hukuku, İstanbul 2014.

Gökcen A., Balcı M., Alşahin M. E., Çakır K., Ceza Muhakemesi Hukuku, Ankara 2018.

Hartung, M., Bues, M. M., & Halbleib, G. (2017). *Legal Tech*. CH Beck.

İçer Z., Suça Teşebbüste Hazırlık Hareketleri İle İcra Hareketlerinin Birbirinden Ayrılması Meselesi", Marmara Üniversitesi Sosyal Bilimler Enstitüsü, (Yayınlanmamış Doktora Tezi), İstanbul 2017.

Katz, D. M., Bommarito II, M. J., & Blackman, J. (2017). A general approach for predicting the behavior of the Supreme Court of the United States. *PloS one*, *12* (4).

Krey V., Deutsches Strafverfahrensrecht, Band 1, Stuttgart 2006.

McCarthy J., What is artificial intelligence? Computer Science Department, Stanford University. Available from: http://www-formal.stanford.edu/jmc/whatisai.pdf (e.t.:20.08.2019)

Ostendorf H., Strafprozessrecht, 1. Auflage, Baden-Baden 2012.

Özbek V. Ö., Doğan K., Bacaksız P., Tepe İ., Ceza Muhakemesi Hukuku, 11. Baskı, Ankara 2018.

Öztürk B. vd., Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, 12. Baskı, Ankara 2018.

Roxin C., Schünemann B., Strafverfahrensrecht, 27. Auflage, München 2012.

Ruger, T. W., Kim, P. T., Martin, A. D., & Quinn, K. M. (2004). The Supreme Court forecasting project: Legal and political science approaches to predicting Supreme Court decisionmaking. *Columbia Law Review*.

Schmid N., Strafprozessrecht, Zürich 1989.

Soyaslan D., Ceza Muhakemesi Hukuku, 5. Baskı, Ankara 2014.

Sözüer A., Suça Teşebbüs, İstanbul 1994.

Şahin C., Ceza Muhakemesi Hukuku I, 9. Bası, Ankara 2018.

Şahin C., Göktürk N., Ceza Muhakemesi Hukuku II, 7. Bası, Ankara 2018.

Turing, A. M. (2009). Computing machinery and intelligence. In *Parsing the Turing Test* (pp. 23-65). Springer, Dordrecht.

Ünver Y., Hakeri H., Ceza Muhakemesi Hukuku, 10. Baskı, Ankara 2015.

Volk K., Grundkurs StPO, 7. Auflage, München 2010.

Yenidünya C., İçer Z., Ceza Muhakemesi Hukuku, Ankara 2016.

Yenisey F., Nuhoğlu A., Ceza Muhakemesi Hukuku, 6. Baskı, Ankara 2018.

Çevrimiçi Kaynaklar

http://ravellaw.com

http://www.dijitalhabitat.com/robotlarin-denetimi-icin-kara-kutu-onerisi/

http://www.hurriyet.com.tr/avrupa/azinlik-raporu-filmi-gercek-oluyor-sucu-islenmeden-onleme-donemi-basliyor-41035280

http://www.hurriyet.com.tr/teknoloji/cinde-mahkemelerde-yapay-zeka-yargic-donemi-41257582

http://www.milliyet.com.tr/teknoloji/ingiliz-polisi-sucu-onlemek-icin-yapay-zeka-kullanacak-2786584

https://fintechistanbul.org/2017/12/26/finansal-suclari-engellemek-icin-yapay-zeka-devrede/

https://intraspexion.com

https://kirasystems.com/

https://lexmachina.com

https://medium.com/@nfo94/black-mirror-subjectivity-and-technology-in-the-entire-history-of-you-e775bfd4640f

https://premonition.ai

https://t24.com.tr/haber/yapay-zeka-yarin-obur-gun-nasil-davranacak-bilemiyoruz,589739

https://turbopatent.com/smartshell/

https://twitter.com/valaafshar/status/934143443886133250?ref_src=twcamp%5Eshare%7Ctwsrc%5Eios%7Ctwgr%5Enet.whatsapp.WhatsApp.ShareExtension%7Ctwcon%5E7100%7Ctwterm%5E0

https://www.anaqua.com/corporate/products/anaqua-studio

https://www.bbc.com/news/uk-48315979

https://www.bbc.com/turkce/haberler-40038611

https://www.bbc.com/turkce/haberler-dunya-44865198

https://www.bloomberg.com/news/articles/2017-02-28/jpmorgan-marshals-an-army-of-developers-to-automate-high-finance

https://www.forbes.com/sites/jasonbloomberg/2018/09/16/dont-trust-artificial-intelligence-time-to-open-the-ai-black-box/

https://www.hitachi.eu/tr-tr/sosyal-inovasyon-hikayeleri/teknoloji/teknoloji-suca-karsi-savasta-gizli-silahimiz

https://www.hukukmedeniyeti.org/haber/20192/hukuk-bilgi-sistemi-hukuk-work-yay-n-hayat-na-ba-l/

https://www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met-police-face-cover-man-fined-a8756936.html

https://www.lawgeex.com/resources/aivslawyer/

https://www.leverton.ai/

https://www.log.com.tr/cin-yapay-zeka-tarafindan-yonetilen-insansiz-polis-istasyonu-hazirliginda/
https://www.mirror.co.uk/tv/tv-news/blackmirror-thirdepisode-theentirehistoryofyou-12260563
https://www.neotalogic.com/product/perfectnda/
https://www.trademarknow.com/
https://www.turklex.com/hukuki-analiz/
https://www.webtekno.com/turkiye-deki-yargitay-davalarini-dogru-tahmin-eden-yapay-zeka-gelistirildi-h58904.html

Yaratan Zeka: Yapay Zeka Tarafından Üretilen Sanat Eserlerinde Eser Sahipliği ve Telif Hakkı Sorunu

Ceren Özbek

1. Giriş

Yapay zeka programları gün geçtikçe daha hızlı, daha yetenekli ve daha karmaşık bir hale gelmektedir. Yapay zeka bazlı çözümler insanların yapabildiği çoğu aktiviteyi, ulaşabildikleri ve işleyebildikleri geniş veri tabanları sayesinde tek başlarına ve kusursuz yapar hale geldiklerinden fazlasıyla tercih edilmektedirler. İş süreçlerinin otomasyonlaşması ve hizmetlerin bireyselleşmesi kısa zamanda daha da yaygınlaşacaktır. Yapay zekaların dahil olduğu yaratım sürecinde halen insan entelektüel zekasına ihtiyaç duyulsa da bu programların söz konusu süreçteki payının arttığını söylemek mümkündür.

Burada ortaya çıkan sorun geleneksel telif hakkı koruma standartlarının pek çok hukuk düzeninde eser sahibinin bir "gerçek kişi" olmasını gerektirmesidir. Ancak teknolojinin gelişimi ile doğan bazı sorunlar göstermektedir ki mevcut yasal düzenlemeler dijital dönüşüm için yeterli değildir. Daha az insan katkısı otonom ve hızlı bir yaratım sürecine yol açacak, fakat geleneksel korumanın gerekleri yerine gelmediğinden birçok eser koruma dışı kalabilecektir. Yapay zeka teknolojisine yapılan yatırım arttıkça hukuksal düzlemde korumasız kalan eserler, bu endüstrinin gelişimine yönelik olan teşvikin azalmasına sebep olacaktır. Bu belirsizlikler nedeniyle eser sahipliği kavramının kapsamı yeniden tanımlanarak, gerektiği takdirde bu yeni nesil sanat eserleri için yeni bir model geliştirilmesi gerekebilecektir.

Bu tebliğde ilk olarak yapay zekanın gelişimi kapsamında bir araç olarak kullanılırken artık otonom şekilde yaratabilen bağımsız bir yaratıcı haline dönüşümü incelenecektir. Devamında şu anki geleneksel telif hakkı korumasının yapay zeka tarafından yaratılan eserler bakımından gerekliliği tartışılacaktır. Eser sahipliğinin geleneksel telif hakkı normları çerçevesinde kendi kendine yaratan bir yapay zekaya verilip verilemeyeceğine ve bu kapsamda çıkabilecek sorunlara yer verilecektir. Günümüzde yapay zeka tarafından üretilen çoğu eserde halen insan katkısı bulunmaktadır. Dolayısıyla bu esere katkıda bulunan farklı kişilerin telif hakkı bakımından sınırları ve bu hakkın taraflar arasında nasıl paylaşılacağı sorunu ele alınacaktır. Son olarak ise telif hakkının sınırlarına ilişkin karşılaştırmalı hukuktaki farklı yaklaşımlar ve alternatif modeller incelenecektir.

[*] İstanbul Üniversitesi Hukuk Fakültesi, Lisans; Queen Mary University of London, Yüksek Lisans.

2. Yapay Zeka Kavramı ve Gelişimi

2.1. Yapay Zekanın Araç Olarak Kullanılması

Yapay zekaya ait disiplinler (tanımlama, öğrenme, değişme, iletişim kurabilme, yaratma vb.) geliştirilirken mümkün olduğu ölçüde insan bilişine en yakın derecede çalışmaları hedeflenmektedir. Yani yapay zekâ geliştirilirken ironik bir şekilde yine insan esas alınmaktadır. Örneğin, bir yapay zekada yer alan dil işleme sistemlerinin bir insana doğal şekilde cevap verebilmesi için çalışılmaktadır. Bu teknik disiplinler Alexa veya Siri gibi robot asistanlarında görüldüğü gibi karşımıza birleştirilmiş bir sistem içinde çıkabileceklerdir. Böylece bu sistemler kullanıcının ihtiyaçları doğrultusunda tasarlanabilmektedir. Aslında bu durum göstermektedir ki tek bir yapay zeka tanımından bahsedilmesi pek mümkün değildir.

Yakın zamana kadar yapay zeka sistemleri henüz öğrenme ve tahmin edilemeyen sonuçlar ortaya koyma yeteneğinden yoksundular. Eserin son hali tamamıyla tahmin edilemese de eserin yaratımında doğrudan insan eli mevcuttu ve insanın söz konusu eserin son haline ilişkin bazı öngörüleri bulunmaktaydı. Bu anlamda bazı yapay zeka sistemleri gerçekten de doğrudan ve sadece insan tarafından kullanılan bir araçtan farksızdırlar. Akla gelen soru bir yapay zeka sisteminin aynen kamera gibi sadece bir araç olarak kullanıldığında onu kullanan kişinin telif hakkı korumasından yararlanıp yararlanamayacağıdır. Bu sorunun cevabı aşağıda tartışmaya açılacaktır.

2.2. Yaratan Zekalar

Bahsedilen yapay zeka sistemleri insan beyni gibi bilgi depolayarak, beyindeki nöronlar gibi çalışabilmekte ve depolanan veriler arasında rastgele bağlantılar ve benzerlikler bulabilmektedirler. Zaten bu rastlantısallık, yapay zeka sisteminden çıkan bu eserin yaratıcısına ya da herhangi bir gerçek kişiye atfedilememesine neden olmaktadır. Bu noktada artık yapay zekayı **"yaratan zeka"** olarak ifade etmenin daha doğru olacağını düşünmekteyiz. Zira yapay zeka, makine öğrenmesi sayesinde kendi hata ve tecrübelerinden yeni sonuçlara ulaşmakta ve adeta bir **yaratan zeka**ya dönüşmektedir. Sistem, kendisi için bir hedef belirlendikten sonra hedeflenen aksiyonu icra edene kadar rastgele denemelerde bulunmaktadır. Sonrasında ise aynı ya da benzer sonucu alana kadar bu aksiyonu tekrarlamaktadır. Sonuç olarak, gelişmiş yapay zeka sistemleri resim yapabilmeyi, yazı yazabilmeyi, beste yapabilmeyi öğrenebilmektedir. Bu doğrultuda ortaya çıkan eser tamamı ile insan entelektüel zekasının sonucu olmayan bir eserdir.

Yapay zeka sistemlerinin ortaya çıkan esere yaptıkları entelektüel katkı üç adımda

gerçekleşmektedir. Öncelikle algoritma için gerekli çeşitli veri örnekleri sınıflandırılır. İkinci olarak bu algoritma yüklenen veriyi küçük elektronik sinyallere böler ve saklanmış benzerlikleri, modelleri ve bağlantıları tespit eder. Bu aşamada verilerde nereye odaklanması gerektiği algoritmaya programlanmamıştır. Ancak yakın zamanda uzmanlar sistemin hedeflenen davranışları daha hızlı gerçekleştirebilmesi için sisteme örnekler gösterilmesinin daha faydalı olacağını fark etmişlerdir. Üçüncü adımda ise sistemin performansı deneyim ve yeni veri girişi ile geliştirilmektedir. İnsan eliyle yüklenmiş olsun veya olmasın veriler arasındaki bağlantıları bulan yapay zeka sistemi bu sayede orijinal ve tahmin edilemeyen sonuçlar, hikayeler, resimler, besteler, tasarımlar ortaya koyabilmektedir. Aslında sadece bir araç olarak ortaya çıkan yapay zekanın giderek kendi kendine yaratan bir zekaya dönüşmesi gelecekte nasıl gelişeceğinin ve otonomlaşacağının habercisi olarak görülebilir.

3. Korumanın Gerekliliği ve Faydaları

Hukuk düzenindeki yeri eş zamanlı olarak şekillenmeye başlayan bu teknolojinin gelişimi birçok soruyu beraberinde getirmektedir. Aslen hukuk düzeni yapay zeka sistemleri ile henüz bütünleşememiştir. Şu anki belirsizlik göz önünde bulundurulduğunda ise gelişmekte olan bu teknolojinin korumadan yoksun bırakılması halinde, bu durumun gelecek yatırımların teşvikini engelleyeceği ileri sürülmüştür. Bunun nedeni belirsiz hukuki korumanın yeni gelişen bu sektör bakımından riskli bir gelişme ortamı yaratmasıdır. Yapay zeka tarafından yaratılan eserlerin direk olarak kamuya açık bir alanda (public domain) yer alması ise bu teknolojiye katkı sağlayan yaratıcıların ve yatırımcıların zamanla yapay zeka gelişim sürecine katılımlarını sınırlandırmalarına yol açabilir.

Telif hakkının amacı yaratıcılara ve eser sahiplerine teşvik ve motivasyon sağlamanın yanında, bu kişilerin yaptıkları çalışmaları ödüllendirmektir. Ancak kendi kendine yaratabilen bir yapay zekanın böyle bir teşvike ihtiyacı olup olmayacağı ise şüphelidir. Yapay zeka teknolojisinin performansı çoğu zaman aldığı somut bir mükafata bağlı değildir. Teknolojinin gelişimi bakımından önem teşkil eden en önemli nokta ise yazılımcılar ve yatırımcılar tarafından bu teknolojinin ilerlemesine finansal destek sağlanmasıdır. Bu yatırımlar devam etmediği sürece yapay zeka teknolojisi ulaşılabilir olmayacaktır.

Yapay zekanın günümüzdeki fikri mülkiyet sistemine uyarlanabilmesi için ülkelerin benimsedikleri yaklaşımların değerlendirilmesi gerekmektedir. Amerikan telif hakkı sistemi orijinal yaratıcıların özellikle münhasır ekonomik haklarını koruyan faydacı bir yaklaşım benimsemektedir. Sözleşme korumasından daha geniş bir koruma sağlamanın sanatın ve bilimin gelişimine katkı sağlayacağı kabul edilmiştir. Bu sayede eser sahipleri yaratarak, geliştirerek ve bu yarattıkları eserleri paylaşarak toplumun refahına daha çok hizmet edeceklerdir. Fikri haklar özellikle Kara Avrupası hukuk sistemlerinde sadece mali menfaatler

değil, eser sahibinin kişiliğine bağlı şahsi menfaatleri de koruma altına almaktadır. Aslında yapay zeka sistemleri tarafından yaratılan eserler ile yaratıcı arasındaki ilişki bazı hallerde çok kolay tespit edilemeyeceği için fikri mülkiyet korumasını meşrulaştırmaya yetmeyecektir.

Sağlıklı bir koruma sistemi gelişmekte olan ülkeler bakımından yabancı yatırımcı çekmek amacıyla da kullanılabilecektir. Bu anlamda yapay zeka yazılımcıları ve yatırımcılarına sürdürülebilir bir güvence sağlamak ve sektörün gelişimi adına telif hakkı koruması sağlamak mantıklı bir çözüm olabilecektir. Bağımsız programcılar yapay zeka tarafından geliştirilen eserler bakımından telif hakları kapsamında büyük şirketlerle daha kolay yarışabilecektir. Buna karşın fazla koruma inovasyon ve sürekliliği engelleyebilecektir.

4. Yapay Zeka Telif Hakkı Sahibi Olabilir mi?

Varlığı açıkça kabul edilmiş olmasa da insan dışında bir eser sahibinin olmasını yasaklayan bir düzenleme çoğu ülkenin hukuk düzeninde yer almamaktadır. Ancak, örneğin Amerika'daki ünlü Naruto kararı kapsamında bir hayvanın yarattığı eser bakımından telif hakkı sahipliği kabul edilmemektedir. Olayda bir maymun türü olan "makak" tarafından çekilen özçekimin (selfie nin) telif hakkı sahipliğinin kime ait olacağından doğan bir ihtilaf söz konusudur. Amerikalı fotoğrafçının makinesinin kullanıldığı fotoğrafta deklanşöre fotoğrafçı değil; Naruto isimli bir makak basmıştır. Bunun üzerine hayvan hakları organizasyonu olan Hayvanlara Etik Muamele İçin Mücadele Edenler (PETA, People for the Ethical Treatment of Animals) tarafından makak Naruto'un telif hakkı sahibi olduğu iddiasıyla dava açılmıştır. Ancak dava sonucunda telif hakkının insan dışındaki varlıklara genişletilemeyeceği gerekçesiyle eserin kamunun kullanımına açık olacağına karar verilmiştir. Aynı zamanda Birleşik Devletler Telif Hakkı Ofisi yayınladığı listede bir maymun tarafından çekilen fotoğrafın telif hakkına haiz bir eser olmadığına dikkat çekmiştir.

Fikir ve Sanat Eserleri Kanunu (FSEK) bakımından eser madde 1/B-(a) uyarınca,"*Sahibinin hususiyetini taşıyan ve ilim ve edebiyat, musiki, güzel sanatlar veya sinema eserleri olarak sayılan her nevi fikir ve sanat mahsullerini… ifade eder*". FSEK kapsamında eser olma, sahibinin özelliğini taşıma ve kanunda sayılan eser kategorilerinden birine dahil olma şeklinde iki şarta bağlanmıştır. Her fikri ürünü bir eser saymak ve korumadan faydalandırmak gereksizdir. Bunun nedeni fikri hakların sağladıkları yetkiler üçüncü şahıslar tarafından toplumun kültürünü zenginleştiren ve ona katkıda bulunan fikrin kullanılmasını kısıtlayacaktır. Seçenekleri yapay zekanın belirlediği veyahut onu kullanan herkesin aynı sonuca yönlendirildiği bir sistem vasıtasıyla meydana getirilen ürün FSEK kapsamında bir eser olarak nitelendirilemez. Yine tesadüfen ortaya çıkan bir ürünün de eser sayılması mümkün değildir.

Eser sahipliği FSEK çerçevesinde bir yaratma fiiline bağlanmıştır. Bu hususiyet dolayısıyla

gerçek kişiler dışındakilerin bir eser sahipliği sıfatına sahip olmasının kabul edilmediği söylenebilecektir. Çünkü eser sahibi onu meydana getiren kişi olarak kabul edilmiştir. Bu kişi hukuk düzeni tarafından birtakım maddi ve manevi hak ve yetkilerle donatılmıştır. Tüzel kişiler, eser üzerinde maddi haklara sahip olabilirken manevi haklardan yararlanamayacaktır. Aynı zamanda eser yaratma kavramının maddi bir fiil olduğu kabul edildiğinden bir tüzel kişi bakımından bu şartın yerine getirilmesi mümkün olmayacaktır. Böylece Türk hukuku kapsamında yapay zeka teknolojisine ve onun ürettiği eserlerin hak sahipliği ancak gerçek veya tüzel kişiler bakımından doğacaktır.

Temelinde yapay zekaya hak ehliyeti verilmesi ona birtakım haklar kazandırabilirken hukuki sorumluluklar da yüklemektedir. Başka bir deyişle, gerçek ve tüzel kişilerden ayrı olarak gerçekleştirdiği fiillerin sonuçlarından sorumlu yeni ve otonom bir yapay zeka kişiliğinden bahsedilmesi gündeme gelecektir. Fakat şu anki hukuk düzeninde gerçek kişilerin yanında yer alan tüzel kişiler yapay zeka kişiliğini kapsamına almamıştır. Zaten yapay zeka halihazırdaki bu hukuk düzeninde bir kişiliğe sahip değildir. Gelecekte ise kazanacağı kişilik formu sonucunda sahip olacağı hak ve fiil ehliyetinin sınırları tartışmalıdır.

5. Hakkın Paylaşımı

Ortaya çıkan bazı örnekler yapay zekanın şimdiden insani özellikler taşıdığını göstermektedir. Bu sistemler insan davranışlarını taklit etmektedir. Aslen yapay zeka sistemleri makine okuması (machine learning) diye tabir edilen kendi kendine öğrenme ile gelişmektedir. Sisteme yüklenen veriler birtakım tahminler, analizler ve bazense bir sanat eseri olarak sonuç doğurabilmektedir. Buna verilecek en güzel örneklerden biri ünlü Hollandalı ressam Rembrandt'ın ölümünün 400 yıl sonrasında eserlerinin analizi sonucu ortaya çıkan "Gelecek Rembrandt" (The Next Rembrandt) tablosudur. 2016 yılında yürütülen proje kapsamında ünlü ressamın ışıklandırma teknikleri, fırça darbeleri ve geometrik desenleri veri analizi sayesinde yapay zekanın yeni, yaratıcı ve tamamen bağımsız (orijinallik kriterini sağlayan) bir eser ortaya çıkarmasını sağlamıştır. Bu doğrultuda mühendislik, tarih ve sanat gibi farklı alanlardan uzmanlar bir araya getirilmiştir. Sonucunda ortaya çıkan eseri insan olmayan bir yapay zeka ortaya koymuştur.

Yapay zekanın telif hakkına hiçbir koşulda sahip olamayacağına karar verildiği takdirde geleneksel telif hakkı koruması çerçevesinde potansiyel üç tarafın telif hakkı sahipliğinden bahsedilebilir: yazılımcılar, yapay zeka sistemlerinin sahipleri, büyük şirketler ve yatırımcılar ve son kullanıcılar. Aynı zamanda veri tedarikçileri, veri tabanı yöneticileri, sistem operatörleri de yapay zeka sistemlerine katkı sağlamaktadırlar ancak bu kişiler eser yaratım sürecine doğrudan katkı sağlamamaktadırlar. Ancak aslında yapay zeka tarafından üretilen eserlerin sahipliği bakımından birden çok tarafın katkısı olacağından hak sahipliğinin çakıştığı durumlar olabilecektir. Bu hakkın paylaşımının bu taraflar arasında geleneksel normlara dayalı olarak mı

olacağı yoksa bir değişime mi uğraması gerektiği ise halen tartışmalıdır.

Öncelikle yapay zeka tarafından üretilen eserlerin telif hakkı korumasına alınması topluma olan katkısı ile tespit edilmelidir. Yukarıda bahsedildiği üzere bu her hukuk düzeninde fikri mülkiyet korumasının amacı farklılık gösterebilecektir. Örneğin, Amerikan faydacı yaklaşımında temel hedef finansal teşvik iken Kara Avrupası hukuk düzeninde bu koruma eser sahibinin kişiliğinin ve yaratıcılığının takdir edilmesi gibi farklı bir amaç taşımaktadır. O nedenle eser sahipliğinin farklı hukuk düzenlerinde farklı kişilere verilmesi mümkün olabilir.Yapay zeka tarafından üretilen eserlerin telif hakkı yapay zeka yazılımının programcısına ait olabilirken programın sahibine de ait olabilecektir. Fikri ürünler insanın sahip olduğu akıl ve entelektüel zekasını kullanarak gerçekleştirdiği çalışmaları neticesinde düşüncenin ürünü olarak ortaya koyulan gayri maddi nitelikte ürünler olarak tanımlanmaktadır. Bu ürünler reel dünyada somutlaştığı halinden farklı bir hukuki rejime tabidir. Örneğin bir kitap olarak karşımıza çıkan hikaye fikri materyalinden bağımsız bir korumaya sahiptir. Böylece bir kitap satın alan kimse yalnızca kitabın mülkiyetine sahip olmaktadır, yani yaratılan fikirlerin cisimlendiği maddenin mülkiyet hakkının sahibidir. Bu kişi kitabı fikri ürün sahibinden, örneğimizde telif hakkı sahibinden, izinsiz olarak çoğaltır ve dağıtırsa onun fikri haklarını ihlal etmiş olacaktır. Çünkü kitabın korunması eşya hukuku kapsamında iken hikaye fikrinin korunması fikri mülkiyet hukuku kapsamında olacaktır. Bu doğrultuda yapay zeka program sahibinin yapay zeka tarafından üretilen eserlere hiçbir yaratıcı ve entelektüel katkısı olmayacaktır.

Bu anlamda yapay zeka tarafından üretilen eserler bakımından eser sahipliğinin ait olabileceği en büyük adaylardan biri de yapay zeka programı yazılımcılarıdır. Yazılımların ve bilgisayar programlarının telif hakkı kapsamında korunabileceği çok tartışılmış olsa da belirli şartları sağlaması durumunda kabul edilmiştir. Aynı çerçevede yapay zeka yazılımının telif haklarını elinde bulunduran kişinin otonomlaşan yapay zekalar tarafından üretilen eserlerde direk hak sahipliği iddia etmesi ise mümkün olamayacaktır. Çünkü artık tamamıyla otonomlaşan yapay zekaların yaratımın sürecinde yazılımcının katkısı sınırlı olacaktır. Yani aslında ne yapay zekanın program sahibi ne de yazılımcısı insan ya da yapay zeka olan bir üçüncü kişi tarafından üretilen eserlerde hak sahipliği iddia edemeyecektir.

Son kullanıcılar ise, yapay zekanın oluşumunda en az paydaya sahip gruptur, bu nedenle eser sahipliği iddiaları daha zayıf kalacaktır. Bu kullanıcıların telif hakkı korumasından faydalanması sektörün gelişimine ket vurabilir. Aynı zamanda sonsuz sayıda son kullanıcı olabilmesi ihtimalinden dolayı hemen herkes telif hakkı sahibi olacağından dolayı korumanın niteliği düşebilecektir. Sonuç olarak yapay zeka tarafından üretilen eserlerin azalması ve endüstrinin gelişiminde düşüş görülebilecektir. Bu duruma çözüm olarak son kullanıcılar ile yapay zeka programlarının yazılım sahipleri arasında lisans sözleşmesi yapılması yeni gelişen

bu sektöre daha fazla katkı sağlayabilecektir.

6. Hakkın Sınırlarına Farklı Yaklaşımlar ve Alternatif Koruma Modelleri

1988 tarihli İngiltere Telif Hakkı, Tasarımlar ve Patentler Kanunu Bölüm 1(1) a uyarınca orijinal eserler emek, yetenek ya da muhakeme içeren yaratan kişinin entelektüel yaratımını içermelidir. Bu Kanunun 9/(3) Bölümü uyarınca bilgisayar tarafından üretilen edebi, dramatik, müzikal ya da sanatsal çalışmalarda istisnai olarak eser sahibi, eserin yaratılması için gerekli ayarlamaları gerçekleştiren kişi olarak kabul edilmiştir. Bu kuralın, yapay zekanın kullanıldığı çalışmalar bakımından da kabul edilmesi ilgili bu eserin ortaya konması için gerekli ayarlamaları yapan kişinin eser sahibi olması anlamına gelecektir. Böyle bir kabulün yapay zeka sektörünün büyümesi ve geliştirilmesine katkı sağlayabileceği savunulsa da Avrupa'nın geri kalanındaki tutum genel anlamıyla bilgisayar tarafından üretilen eserler bakımından daha çekimserdir.

İngiltere'deki madde 9(3) gibi bir istisna kabul edilmediğinden Kara Avrupası sistemlerinde bilgisayar üretimi eserlerin fikri mülkiyet kapsamında korunması henüz yeknesak bir şekilde kabul edilmemiştir. Örneğin, **Alman hukukunda** Telif Hakkı Kanunu madde 7 eser sahibinin eserin yaratıcısı olduğu kabul edilse de yine madde 11 telif hakkının eser sahibi ile eserin entelektüel ve kişisel ilişkisini koruduğunu kabul etmiştir. Yine **İspanyol fikri mülkiyet hukuku** eserin sahibinin onu yaratan gerçek kişi olduğunu vurgulamaktadır. Bu nedenle eser sahipliği bakımından eser ile eser sahibinin kişiliği arasındaki sıkı bağlantı temel şarttır. Eserin orijinallik seviyesi ise aynı bağlamda eser sahibinin kim olduğunun ulusal hukuk literatüründe nasıl belirlendiğine bağlı olarak her hukuk düzeninde çeşitlilik gösterecektir. Avrupa Birliği Adalet Divanı tarafından bir eserin orijinal sayılabilmesi *Infopaq* kararı kapsamında "eser sahibinin kendi entelektüel yaratımı" olarak kabul edilmesine bağlanmıştır. Yapay zeka tarafından üretilen eserlerin bu karar kapsamında Avrupa'da telif hakkı kapsamında korunup korunamayacağı orijinallik kıstasına yani o eserin yaratımında insan payının ne kadar olduğuna bağlıdır.

Giderek bağımsızlaşan yapay zeka sistemlerinin üretim sürecinde insanın katkısının olmadığı durumlara Adalet Divanı'nın Infopaq kararında kabul ettiği standart uygulanabilir. Divan, eserin unsurları orijinal olmasa da bu unsurların seçilerek bir araya getirilmesinin de orijinallik şartını yerine getirdiği yorumunu yapmıştır. Örneğin, bir kişinin eseri bir araya getiren orijinal olmayan unsurları seçimi, birleştirmesi ve kombinasyonu onun yaratıcılığını yansıtır ve entelektüel bir yaratım ortaya koyar. Ancak tabii ki yapay zekanın kararların büyük bir kısmını kendisinin verdiği durumlarda bu orijinallik kıstasının yerine getirilmesi mümkün olamayacaktır.

Amerikan hukuk düzeninde iş ilişkisi veya sipariş üzerine yaptırılan eserler kapsamında "work made for hire" olarak adlandırılan doktrin kabul edilmiştir. Bu doktrine göre eser sahipliği ve bundan doğan haklar taraflar arasında aksine yazılı bir anlaşma bulunmadıkça işverene veya siparişte bulunan kişiye ait olacaktır. İşveren bir gerçek ya da tüzel kişi olabilir. Bu modelin hiçbir komut almaksızın kendi kendine bir ürün ortaya koyan yapay zeka tarafından üretilen eserlere hukuki koruma getirme açısından uygulanması önerilmiştir. Bu görüşe göre işveren ve işçi kavramlarının geniş yorumlanması ile yapay zeka sistemi işçi olarak kabul edilebilecektir. Yapay zeka sisteminin yazılımcısı veya sahibinin yaratıcı eserler üretmek için yapay zekayı kullanması durumu işverenin bir amaç doğrultusunda bir işçiyi bir hizmet veya iş kapsamında istihdam etmesi olarak yorumlanabilir. Aynı doğrultuda yapay zeka sistemi görevlendirilen bir işçi olarak kabul edilebilir. İşveren eserin asıl yaratıcısı olmasa da eser sahipliğinin şartlarını yerine getirmiş sayılacağından yapay zekanın ürettiği eserler bakımından telif hakkı iddiasında bulunabilecektir. Söz konusu doktrindeki terimlerin yeniden yorumlanarak bu yeni tip eserlere koruma sağlanması yapay zeka sektörünün gelecekteki gelişimi bakımından teşvik edici olabilecektir.

Türk hukuku kapsamında ise bu modelin uyarlanması pek mümkün gözükmemektedir. Öncelikle Türk hukukunda, işçiler tarafından üretilen eserler bakımından eser sahipliğinin işçilere ait olduğu kabul edilmektedir. İşverene ise sadece mali hakları kullanma yetkisi ait olabilecektir. Yine Türk hukukunda işçi olabilmek için gerçek kişi olma şartı getirilmiştir. Dolayısıyla "work made for hire" kapsamında yapay zekaların daha geniş bir yorumla işçi olarak kabul edilmesinin günümüzde mümkün olmadığı söylenebilir.

7. Sonuç

Ülkelerin ulusal hukuk düzenlemeleri gereği korunan hukuki değerin önceliği farklılık göstereceğinden telif hakkı sahipliği değişik menfaat sahiplerine verilebilecektir. Zaten karşılaştırmalı hukuk incelendiğinde dijital dönüşüm kapsamında telif hakkı korumasının şartlarına ülkelerdeki sosyoekonomik durumlar doğrultusunda bazı istisnalar getirildiği de görülecektir. Yine hâlihazırda telif hakkı korumasının ve eser sahipliğinin belirlenmesi için kullanılan bazı doktrinler bu dönüşüme uyarlanmaya çalışılmaktadır. Özellikle bilgisayarların veya bilgisayar programlarının yaratıcı süreçlere dahil olmasıyla mevcut yasal düzenlemelerin bu sistemlere uyumlu hale getirilmesi istenmiştir. Ancak getirilen çözüm önerilerinin yapay zeka sistemleri bakımından uygulanabilirliği konusunda henüz bir görüş birliği sağlanamamıştır. Zaten giderek bağımsızlaşan yapay zekaların daha değişken ve kapsamlı yasal düzenlemelerle korunması ve geliştirilmesi söz konusu olacağa benzemektedir.

Bibliyografi

Guadamus A, "Do Androids Dream Of Electric Copyright? Comparative Analysis Of Originality İn Artificial İntelligence Generated Works?"[2017] *IP Quarterly,* 2

Bridy A, "Coding Creativity: Copyright and The Artificially Intelligent Author" [2012] *Stanford Technology Law Review* 5

C-5/08 *Infopaq International A/S V Danske Dagblades Forening* [2009] EU:C:2009

De Rouck F, "Moral Rights & AI Environments:The Unique Bond Between Intelligent Agents and Their Creations" [2019] *Journal Of Intellectual Property Law & Practice*, 14,4

Deltorn J M / Macrez F , "Authorship In the Age Of Machine Learning and Artificial Intelligence" [2018] Center For International Intellectual Property Studies Research Paper No. 2018-10

Kalin H, "Artificial Intelligence and The Copyright Dilemma" *Idea: The Journal Of The Franklin Pierce Center For Intellectual Property* [2017] 57/3, 431

Kaminski M E, "Authorship, Disrupted: AI Authors in Copyright and First Amendment Law" [2017]
UC Davis Law Review, 51,58

Naruto v. Slater, No. 16-15469 (9th Cir. 2018)

Stephens K /Bond T, " Navigating IP Challenges" [2018] *PLC*

Magazine, 39 Tekinalp Ü, Fikrî Mülkiyet Hukuku, Vedat Kitapçılık, 5.

Baskı, İstanbul, 2012.

Yanisky-Ravid S, "Generating Rembrandt: Artificial Intelligence, Copyright And Accountability In The 3A Era—The Human-Like Authors Are Already Here: A New Model" [2017] *Michigan State Law Review*, 2017/4, 659

Zorluel M, "Yapay Zekâ Ve Telif Hakkı"[2019] TBB Dergisi, 142

SAYISAL DELİLİN DEĞİŞTİRİLEMEZLİĞİNİN SAĞLANMASININ YOLU OLARAK ÖZET DEĞER KAVRAMI VE ÖZET DEĞER ÇAKIŞMASI[1]

Doç.Dr. Olgun DEĞİRMENCİ*

ÖZET

Ceza muhakemesine konu maddi olayı ispatlamak için kullanılan delil, mahkemenin önüne getirilene kadar değiştirilmemelidir. Fiziksel delillerin, adli emanete alınması suretiyle doğruluklarını sağlamak nispeten kolaydır. Bununla birlikte sayısal delillerin kolayca kopyalanabilmeleri ve değiştirilebilmeleri, doğruluklarının sağlanması güçtür. Sayısal delillerin doğruluklarını temin etmek için teknolojik olanaklardan yararlanılmaktadır. Tek yönlü özetleme değeri sağlayan özet değer (hash value), bir parmak izi gibi sayısal delile uygulanabilmekte ve sayısal delilin doğruluğunu sağlamaya yardımcı olmaktadır. Ancak iki farklı sayısal verinin aynı özet değere sahip olması olan özet değer çakışması, sayısal delilin doğruluğunu sağlamada sorunlu bir alandır. Bu çalışmada sayısal delilin doğruluğunu sağlama aracı olarak özet değer kavramı açıklanacak ve özet değerin çakışmasının muhtemel etkilerine değinilecektir.

THE CONCEPT OF HASH VALUE AND THE COLLISION OF HASH VALUE AS THE WAY TO PROVIDE UNASSAILABILITY OF DIGITAL EVIDENCE

ABSTRACT

The evidence used to prove the material fact which is subject to the criminal procedure should not be changed until it is brought before the court. It is relatively easy to ensure the accuracy of physical evidences by taking them into judicial custody. However, it is difficult to ensure that the digital evidence can be easily copied and modified. Digital evindences are used to provide the technological means to ensure accuracy. The hash value, which provides a one-way summarization value, can be applied to digital evidence such as a fingerprint and helps to ensure the accuracy of the numerical evidence. However, a collision of hash value, known as a hash value conflict, with two different digital data having the same hash value, is a problematic area in ensuring the accuracy of numerical evidence. In this study, the concept of summary value as a means of ensuring the accuracy of numerical evidence will be explained and the possible effects of the collision of hash value will be discussed.

I. CEZA MUHAKEMESİNDE DELİL KAVRAMI

Ceza muhakemesinin, *"müşahhas olayın normlar karşısındaki durumunun tespiti meselesi"*[2] şeklinde ele alınması, aslında somut olayın, ceza muhakemesinin belirleme alanının dışında olduğu izlenimi yarattığından dolayı amacı tam olarak ifade etmemektedir. Ceza muhakemesinde temel olarak iki olayın çözümlemesi yapılmaktadır. Bunlardan ilki ve öncelikle çözümlenmesi gereken husus maddi olaydır ki, bu gerçek dünyada muhakemeye konu olayın nasıl gerçekleştiği hususunda, müştereken ancak yargılama makamında makul şüpheden arındırılmış vicdani kanaatin oluşturulması şeklinde ortaya konulur. İkinci olay ise nispeten

---

1 Bu tebliğ Yazarın, Bilgi Toplumunun Delil Türü: Sayısal Delil ve Bilimselliği (*Terazi Hukuk Dergisi*, C.9, S. 97, (Eylül 2014), pp. 14 – 28) ve Yargılama Makamı İçin Şüphe, Müdafi İçin Savunma Nedeni: Adli Bilişimde Özet Değer (Hash Value) Kavramı ve Özet Değer Çakışmasının Ceza Muhakemesine Etkileri (Terazi Hukuk Dergisi, C. 13, S. 137, (Ocak 2018), pp. 120 – 126) makalelerinde yer alan görüşlerinin geliştirilmesi ile oluşturulmuştur.

* TOBB Ekonomi ve Teknoloji Üniversitesi, Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Öğretim Üyesi, odegirmenci@etu.edu.tr

2 Nurullah Kunter**,** *Ceza Muhakemesi Hukuku*, Yenileştirilmiş ve Geliştirilmiş 4'üncü Bası (İstanbul 1970), 33.

çözümü daha kolaydır ve somut olayın, hukuk normları karşısındaki durumunun, yorum yoluyla ortaya konmasıdır.[3]

Maddi olayın çözümü aslında tüm bilimlerin faaliyet alanına girmektedir ki, herhangi bir bilimin başına "adli" (İngilizce forensic) kelimesi getirildiğinde, o bilim disiplini ceza muhakemesine konu maddi olayın çözümü bakımından kullanılabilecektir.[4] Maddi olay, kronolojik olarak muhakemenin duruşma safhasından önce gerçekleştiğinden dolayı, o olaydan günümüze kalanlar ile olay hakkında karar vermemiz gereklidir. Geçmişte yaşanan olay ile ilgili günümüze devrolunan her şey delil kavramı altında incelenmektedir. Elimizdeki deliller ile adeta maddi olayı yeniden oluşturmakta, suçu yeniden yapılandırılmaktayız (crime reconstruction).[5]

Maddi olayın ne şekilde olduğunu anlamamızı sağlayan ve bazı özelliklere sahip olan her türlü araca delil denmektedir.[6] CMK m. 217/1'de, hâkimin kararını ancak delile dayandırabileceği ifade edilmiş ve hâkimin hükmüne esas olabilecek delille ilgili özellikler vurgulanmıştır. Bu noktadan hareketle hâkimin vicdani kanaatinin ancak delile dayandırılabileceği, delilsiz mahkûmiyetin olmayacağı[7], mutlak gerçeğe en yakın maddi gerçeğe ancak delil ile ulaşılabileceği ifade edilmektedir.[8]

Ceza muhakemesinin maddi konusu olan geçmişte yaşanılan olay, tarafların katılımıyla, muhakeme esnasında müşterek olarak yargıcın zihninde yeniden canlandırılacaktır. Başka bir anlatımla maddi gerçek, bugüne dayanılarak dünün öğrenilmesi faaliyeti[9] şeklinde ortaya çıkarılacaktır. Söz konusu canlandırmayı yapan veya başka bir anlatımla, geçmişte yaşanan olayın parçalarını bugüne taşıyan vasıtalar delillerdir.[10] Öğretiye bakıldığında delillerin özelliklerinin genelde şu şekilde ifade edildiği görülmektedir; gerçekçi olması, akla uygun olması, olayı temsil edici olması, hukuka uygun olması ve müşterek olması.[11] Konumuzla ilgili bazı özellikli hususlara kısaca değinilecek, delil kavramına ilişkin sınırlar çizildikten sonra sayısal delil kavramı açıklanmaya çalışılacaktır.

Öncelikle delilin, ceza muhakemesine konu maddi olayı temsil edici niteliği olmalıdır.[12] Delilin temsil ediciliği, maddi olayın bir parçası olması veya maddi olayı yansıtması ile ilgili bir kavramdır.[13] Öğretide bazı yazarlar tarafından delilin sağlamlığı ve güvenilirliği de, bu başlık altında değerlendirilmesine rağmen[14], biz konunun önemine binaen ayrı bir başlık altında değerlendireceğiz.

---

3 Sami Selçuk, "Temyiz Denetiminin Sınırları ve Bu Sınırlara Uymamanın Kaçınılmaz Sancılı Sonuçları/Açmazları/Tehlikeleri", *Marmara Üniversitesi Hukuk Araştırmaları Dergisi*, Prof.Dr. Nur Centel'e Armağan, C.19, S. 2, (İstanbul 2013), 332 (pp. 319 - 361); Cumhur Şahin, *Ceza Muhakemesinde İspat (Delillerin Doğrudan Doğruyalığı İlkesi)*, (Yetkin Yayınları 2001), 19.

4 En bilinenlerinden adli tıp, adli fizik, adli kimya, adli muhasebe, adli teoloji, adli edebiyat vs. Bu konuda bkz. Nedir Bu Adli Bilimler/Kimdir Bu Adli Bilimciler, Adli Bilimciler Derneği Yayını, (Ankara 2019).

5 Bu konuda bkz. W. Berry Chisum – Brent E. Turvey, *Crime Reconstruction*, (Academic Press 2007), XV.

6 Doğan Gedik, *Öğreti ve Yargısal İçtihatlar Işığında Ceza Muhakemesinde Şüpheden Sanık Yararlanır İlkesi (In Dubio Pro Reo)*, (Adalet Yayınevi 2016), 11; Koray Doğan, *Ceza Muhakemesinde Belirsizlik Kuşkudan Sanık Yararlanır İlkesi "in dubio pro reo"*, (Seçkin Yayıncılık 2016), 235; Mehmet Yayla, *Ceza Muhakemesi Hukukunda İspat ve Şüphe*, (Seçkin Yayıncılık 2016), 96.

7 Devrim Aydın, Ceza Muhakemesinde Deliller, (Yetkin Yayınları 2014), 38.

8 Mahmut Koca, "Ceza Muhakemesi Hukukunda Delil", *Ceza Hukuku Dergisi*, C. 1, S. 2 (Aralık 2016), 207 (pp. 207 – 225); Gedik, 12.

9 Cumhur Şahin – Neslihan Göktürk, *Ceza Muhakemesi Hukuku – II*. Gözden Geçirilmiş ve Güncellenmiş 8. Baskı, (Seçkin Yayıncılık 2019), 25.

10 Vahit Bıçak, *Suç Muhakemesi Hukuku*, Genişletilmiş 4. Bası, (Seçkin Yayıncılık 2018) 457; Ali Eryılmaz, *Ceza ve Disiplin Hukukunda Hukuka Aykırı Delil*, (HUKAB Yayınları 2013), 13.

11 Gedik, 12, 13; Koca, 213.

12 Nur Centel – Hamide Zafer, Ceza Muhakemesi Hukuku, 14. Baskı, (İstanbul 2017), 235.

13 Bıçak, 426.

14 Şahin – Göktürk, II, 30.

Deliller, insanların iç dünyalarına değil, dış dünyaya, nesnel alana ait araçlardır. Bu bakımdan deliller maddidirler ve beş duyu organıyla algılanabilecek şekilde maddi bir yapıya sahip olmayan şeyler delil olamayacaktır.[15]

Deliller elde edilebilir veya erişilebilir olmalıdır. Ulaşılma olanağı bulunmayan ispat araçlarının duruşmaya getirilmesi ve tartışmaya açılabilmesi olanağı yoktur.[16]

Deliller hukuka uygun şekilde elde edilmiş olmalıdırlar. Ceza muhakemesinde her şeyin delil olabileceği ilkesi, her türlü yöntemin kullanılabileceği, yasayla gösterilen usul ve esasların göz önünde tutulmadan delillere ulaşılabileceği sonucuna varmamızı sağlamaz.[17]

Deliller güvenilir olmalıdır.[18] Bu kapsamda delilin, elde edildiği andan ceza yargıcının karşısına çıkarılana kadar doğruluğu ve bütünlüğü sağlanmış olmalıdır. Deliller değiştirilmemelidir. Esasen çalışmamızda, delilin bu özelliği ile ilgilidir. Nitekim olay yerinden duruşmaya taşınana kadar, delilin olayı temsil edicilik niteliği zarar görmemeli, delile mahkeme tarafından güvenilmelidir.

Deliller müşterek olmalıdır.[19] Delillerin müşterekliği duruşmada tartışılmak suretiyle sağlanacaktır. Delillerin duruşmada tartışılabilmesi için tarafların delillere ulaşabilmesi veya delillerin taraflara bildirilmesi (CMK m. 179, 181) gereklidir.[20] Yargıç, kararını ancak duruşmaya getirilen ve huzurunda tartışılan delillere dayandırabilecektir. Her bir delil bakımından davanın taraflarına, söz konusu delili çürütebilme, delile ilişkin düşüncelerini açıklayabilme hakkı verilmelidir.

Deliller akılcı ve bilimsel olmalıdır.[21] Akılcılık, önyargılardan sıyrılmış bir şekilde, mantık biliminin ilkelerinden hareketle sonuca varılmak suretiyle belirlenecektir.[22] Akla uygun olmayan deliller muhakemede kullanılamaz.[23]

II. DELİL TÜRÜ OLARAK SAYISAL DELİL VE ÖZELLİKLERİ

Sıklıkla ifade edildiği gibi, *"nerede toplum varsa orada hukuk vardır"* (Ubi societas ibi jus)[24] deyişinin, bilgi toplumuna dönüş ile beraber evrildiği ve *"toplum nereye yoğunlaştıysa, hukuk da oraya yoğunlaşmalıdır"* şekline dönüştüğü kanaatindeyiz. Toplumsal hayatta, bilişim sistemlerinin daha fazla kullanılır olması, toplumun oraya yoğunlaşmasına neden olmaktadır. Toplumun yarattığı bir olgu olan suç da, doğal olarak bilişim sistemlerine yoğunlaşmaktadır. Suçun ispatı için kullanılacak delillerin de, suçun yoğunlaştığı yerde aranması gerekliliğinden dolayı sayısallığa evrildiğini söyleyebiliriz. *"Suç sayısallaşmaktadır"*[25], ifadesi; suç ve delil sayısallaşmaktadır şekline kolaylıkla çevrilerek okunabilir.

---

15 Centel – Zafer, 235; Şahin – Göktürk, II, 30.

16 Centel – Zafer, 235; Şahin – Göktürk, II, 30.

17 Bkz. Claus Roxin, "İspat Hukukunun Esasları" (Çeviren Yener Ünver), *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, Y.4, S.8, (Güz 2005), 273.

18 Centel – Zafer, 235.

19 Centel – Zafer, 235.

20 Centel – Zafer, 235.

21 Centel – Zafer, 235; Tosun, delillerin tarihsel akış içinde akıldışı ve akılcı olmak üzere iki aşamadan geçtiğini ifade etmiştir. Yazara göre insanlar uzun yıllar akıl dışı delillere itibar etmişlerdir. Mesela sanığın elini kızgın yağa sokmak suretiyle anlatımlarının doğruluğunu denetlemişlerdir. Zamanla akılcı deliller aşamasına geçilmiştir (Tosun, Öztekin, *Türk Suç Muhakemesi Hukuku Dersleri*. C.:1, (İstanbul: 1984), 713 vd.); Feyzioğlu, ispat sistemi safhalarını; etnik safha, dini safha, kanuni safha, vicdani safha olarak tasnif tabi tutmak suretiyle incelemiş ve bilimsel ispatın mümkün olup olmadığını tartışmıştır (Metin Feyzioğlu, *Ceza Muhakemesinde Vicdani Kanaat*. (Ankara: 2002), 38 vd.).

22 Bıçak, 429.

23 Delilin bilimselliği konusunda ayrıca bkz. Olgun Değirmenci, "Bilgi Toplumunun Delil Türü: Sayısal Delil ve Bilimselliği", *Terazi Hukuk Dergisi*, C.9, S. 97, (Eylül 2014), pp. 14 – 28.

24 Bkz. Ahmet Ulvi Türkbağ, "Hukuka Gerçekçi Eleştirel Bakış: Hukuk Sosyolojisi", Sosyoloji Dergisi, 3. Dizi, 16. Sayı, 2008/1, 43 – 54.

25 John E.D. Larkin "Compelled Production of Encrypted Data", *Vanderbilt Journal of Entertainment and Technology Law*, Vol. 14, Number 2, (Winter 2012), 254.

Sayısal delil, sayısal ortamda tutulan, oluşturulan, depolanan, iletilen her türlü veridir. Sayısal delilin esası veri olmasıdır. Her veride olduğu gibi sayısal delil de temelinde 1 ve 0 şeklinde bitlerden oluşmaktadır.[26] Ancak söz konusu veriye, delil niteliği kazandıran ceza muhakemesine konu olan maddi olayla ilgisinin bulunmasıdır. Teknik açıdan sayısal delil, verinin durumu veya sayısal vaka hakkında bir hipotezi destekleyen veya çürüten her türlü veri olarak tanımlanmaktadır.[27]

Sayısal delil; bilgisayar programları, bilgisayar ağları veya diğer elektronik cihazlarda bulunabilmektedir.[28] Sayısal delil, bulunduğu ortamda çeşitli şekillerde varlık gösterebilir. Örneğin bir ticari işlemin belgesi olarak işlem sırasında oluşturulabilir. Bir belge olarak sayısal ortamda bulunabilir veya görsel/işitsel kayıt olarak uygun ortamda yer alabilir.[29] Günümüzde toplumsal hayatın her alanındaki işlemlerin mutlaka bir sayısal yönünün olduğunu söyleyebiliriz. Bunlara; sağlık kayıtlarından, bina yapım projelerine, eczaneden aldığınız ilacın bilgilerinden, çocuğunuzun bakımını üstlenen gündüz bakımevindeki kayıtlara kadar çok geniş bir alan dâhildir.[30] *Casey*'in ifade ettiği gibi günümüzde hemen hemen her vaka, bir yönüyle elektronik posta bağlantılı çözülmektedir.[31] Sayısal delilin, sadece bilişim suçları ile ilgili olayların değil, hemen hemen her türlü olayın aydınlatılmasında kullanılır hale gelmesi de, öneminin gün geçtikçe artmasına neden olmaktadır. Sayısal delilin ceza muhakemesinde de önemi artmakta, ceza davalarının en önemli delillerinden biri olmaktadır.[32] Bazı davalarda, örneğin çocuk pornografisi eylemlerinde, olayı bir adım daha ileriye götürerek, sayısal delil haricinde bir delile ulaşmanın olanaksız olduğu da ifade edilmektedir.[33]

Sayısal delil kavramı karşımıza öncelikle bilgisayar delili olarak çıkmıştır. Bu dönemlerde bilgisayar delilinden anlaşılan bilgisayarda yer alan bir dosyanın çıktısıdır. Ancak teknolojinin gelişimi ile beraber bilgisayar delili kavramının yerini sayısal delil almıştır. Kavramla ifade edilen de, artık sadece bir yazıcı çıktısı değil, insan veya sistem tarafından üretilip üretilmediğine bakılmaksızın bilişim sistemlerinde, depolama birimlerinde depolanan, işlenen, aktarılan tüm bilgiler olmuştur.[34]

Sosyal medyanın (Twitter, Facebook ve MySpace vb.) gelişimi ile beraber, insanlar günlük faaliyetlerini, kişisel görüntülerini, düşüncelerini ve bulundukları yerleri başkaları ile paylaşmaya başlamışlardır. Günlük faaliyetlerin paylaşılması ile gerçek hayat, sayısal olarak bilişim sistemlerine kaydedilmiş olmaktadır. Bunun yanı sıra *"blogların"* artması ile beraber insanlar bir gazeteci gibi düşüncelerini ve günlük olaylarla ilgili görüşlerini yazmakta, kendi yayın organlarını oluşturmaktadırlar.[35] Teknolojinin tüm bu çıktıları, toplumu ve toplumdan

---

26 Christina M. Schuck, "A Search for the Caselaw to Support the Computer Search 'Guidance' in United States v. Comprehensive Drug Testing", *Lewis & Clark Law Review*, Vol. 16, No. 2, (2012), 749.

27 Nikpi O. Ademu – Chris O. Imafidon – David S. Preston, "A New Approach of Digital Forensic Model for Digital Forensic Investigation", *International Journal of Advanced Computer Science and Applications*, Vol. 2, No. 12, (2011), 175; Benzer bir tanım için bkz. Eoghan Casey, *Digital Evidence and Computer Crime*. Second Edition, (USA: Academic Press, 2004), 12.

28 Wayne Jekot, "Computer Forensics, Search Strategies, and the Particularity Requirement", *Pittsburgh University Journal of Technology Law and Policy*, Vol. VII, (Spring 2007), 6.

29 Larry Daniel – Lars Daniel, *Digital Forensics for Legal Professionals Understanding Digital Evidence From The Warrant To The Courtroom*. (USA: Syngress, 2012), 4.

30 Daniel – Daniel, 4.

31 Yazar bu görüşü*; "uğraştığımız hemen hemen her olay, dumanı tüten bir elektronik posta unsuruna sahiptir"* şeklinde ifade etmektedir (Eoghan Casey, "Reconstruction Digital Evidence", in: *Crime Reconstruction* (Edited by W. Jerry Chisum – Brent E. Turvey), (2006), 419, 420).

32 Susan Brenner tarafından internet günlüğünde ifade edilmiştir. Bkz. http://thinkexist.com/quotes/susan_brenner/, Erişim Tarihi: 01 Şubat 2014.

33 Digital Evidence in the Courtroom: A Guide for Preparing Digital Evidence for Courtroom Presentation, The National Center for Forensic Science, 2003, http:/www.ncfs.org/DE_courtroomdraft.pdf, Erişim Tarihi: 10.09.2011.

34 Schatz, 1.

35 Daniel – Daniel, 4.

kaynaklanan suçu, dolayısıyla da suç delillerini fizikselden sayısala doğru hareketlendirmektedir.

Sayısal deliller birtakım özelliklere sahiptir. Öncelikle gözle görülemez ve gizli niteliktedir. Sayısal delillerin varlığının anlaşılabilmesi, analog veya fiziksel delillerden farklı olarak yardımcı alet veya teçhizat ile mümkün olmaktadır.[36] Söz konusu teçhizat; donanım ve yazılımdan oluşmaktadır. Örneğin bir kelime işlemci dosyasında bulunan veriyi görebilmek, yazıcıdan çıktı almak veya ekran vasıtasıyla mümkün olabilecektir. Sayısal delillerin; bilgisayar çıktısı veya ekran çıktısı olması durumunda, söz konusu veri ile beraber saklanan verinin verisi olarak tanımlanan üst verileri (metadata)[37] görmek mümkün olmayacaktır.[38] Bu bağlamda sayısal veriyi, insan için anlaşılabilir kılan her araç, söz konusu sayısal verinin ancak bir kısmı hakkında bize bilgi verebilir. Sayısal deliller hakkında oluşturulma, kopyalanma veya değiştirilme zamanları gibi birçok önemli bilgileri barındıran üst verilerin çıktılarda görülememesi[39], delili değerlendiren makamlar bakımından büyük eksiklik olarak ortaya çıkmaktadır. Ancak belirtelim ki, sayısal delillerde, delil niteliğinde olan ekrandan veya yazıcıdan alınabilen çıktı değil, bizzat sayısal ortamdaki verinin kendisidir.[40] Dolayısıyla sayısal ortamdaki verinin kendisi olduğu için söz konusu veri hakkında bize bilgi veren üst veriler de sayısal delilin kapsamındadır.

Sayısal deliller hassas bir yapıya sahiptirler. Delilin olay yerinden toplanmasında birtakım kurallara riayet edilmemesi delillerin kaybı ile sonuçlanabileceği gibi delillerin tahrifine de neden olabilecektir.[41]

Sayısal delillerin tahrif edilebilmesi olanağı, delilin güvenilirliği sorununu da beraberinde getirmektedir. Avrupa Birliğine üye ülkelerde yapılan bir çalışma delillerin güvenilirliği konusunda yargıçlar arasında bir görüş birliği olmadığını ortaya çıkarmaktadır. Nitekim bazı yargıçlar nesnel ve kesin olduklarından dolayı elektronik delillerin daha güvenilir olduğu ve yargılamada kullanılması kanaatini taşımaktadırlar. Buna karşılık diğer bazı yargıçlar, elektronik delillerin sahihliğini doğrulamanın güçlüğünden hareketle klasik delillere göre daha fazla istismara açık ve daha az güvenilir olduğunu düşünmektedirler.[42]

Sayısal delillerin anlam kazanabilmesi ancak bilişim sisteminin bir bütün olarak incelenmesi ile mümkündür. Sayısal delillerin, fiziksel delillerden farklı olarak bütünden ayrı olarak incelenmesi, sayısal delilin olayı temsil edici niteliğini ya yitirmesine neden olacak ya da büyük ölçüde kaybettirecektir. Sayısal delillerin doğrulanması, sistemin tamamen incelenmesi veya başka bir kaynaktan teyidi ile mümkündür. Örneğin bir elektronik postanın doğruluğunun, servis sağlayıcıları vasıtasıyla teyit edilmesi bu duruma örnek olarak verilebilir.[43]

Sayısal deliller, bulunduğu ortamda olayla ilgili olmayan verilerle karışık bir halde bulunmaktadır. Bir disk sürücüde bulunan verilerden küçük bir kısmı ceza muhakemesine konu

---

36 Göksu, 30; Peter Sommer, "Downloads, Logs and Captures: Evidence from Cyberspace", Journal of Financial Crime, Vol. 5, 142.

37 Üst veriler, bir belgenin tarihçesi gibidir. Belgeye yapılan her girdi, ilgili belgede kaydedilir (Adam Israel, "To Scrub or Not to Scrub: The Ethical Implications of Metadata and Electronic Data Creation, Exchange, and Discovery, Alabama Law Review, Vol. 60, (2009), 472, 73).

38 J. Brian Beckham, "Production, Preservation, and Disclosure of Metadata", *The Columbia Science and Technology Law Review*, Vol. VII, (2006), 3; Philip J. Favro, "A New Frontier in Electronic Discovery: Preserving and Obtaining Metadata", *Boston University Journal of Science and Technology Law*, Vol. 13, Issue 1, 4; Melise R. Blakeslee, *Internet Crimes, Torts and Scams, Investigation and Remedies*. (New York: Oxford University Press, 2010), 216.

39 Üstveriler; belgeyi hazırlayan kişiyi, belgenin hazırlandığı zamanı, belge üzerinde değişiklik yapan son on kişinin listesini, belgenin gözden geçirildiği zamanı, belgedeki değişiklikleri ve diğer bilgileri bize sağlayabilir (Favro, 7; Beckham, 2 vd.). Bu belgelere bazı durumlarda ağ sunumcusunun ismi, belgenin sabit diskte kaydedildiği yer gibi ceza soruşturması bakımından önemli kabul edilen bilgiler de dâhildir (David Hricik, "The Transmission and Receipt of Invisible Confidential Information", http//www.hricik.com/eethics/Metadata1103.doc, Erişim Tarihi: 06 Ocak 2013).

40 Göksu, 30.

41 Ünal, 17; Ademu – Imafidon – Preston, 175.

42 Insa, 29.

43 Göksu, 31.

olayla ilgili olabilmektedir. Olayla ilgili olan sayısal verilerin bulunması, çıkarılması ve anlaşılabilir hale getirilmesi gereklidir.[44] Bu durum ise sayısal verileri, delil haline getirecek kişilerin, bu hususta uzmanlaşması ile mümkün olacaktır. Uzmanlaşmanın yanı sıra zaman faktörü de, sayısal verinin sayısal delil haline dönüştürülmesi sürecini etkileyen önemli faktörlerden birisidir. Sayısal delilin elde edilmesi ayrıca zaman alıcı bir faaliyet olarak karşımıza çıkmaktadır.

Fiziksel delillerin, delilin incelenmesi ile tükenme olanağı mevcuttur. Bununla birlikte sayısal deliller kolaylıkla birebir kopyalanabilmekte ve kopyası üzerinden gerçekmiş gibi işlem yapılabilmektedir. Uygulamada sayısal delillerin incelenme işlemi kopyaları üzerinden yapılmaktadır.[45]

Sayısal deliller tahrife, fiziksel delillerden daha fazla açıktırlar.[46] Sayısal deliller, failler tarafından delillerin karartılması saikiyle tahrif edilebileceği gibi sayısal delilin toplanması sırasında sehven de tahrif edilebilirler.[47]

Sayısal delillerin, fiziksel delillerden farklı olarak tamamen yok edilmesi ancak onu barındıran fiziksel ortamın geriye döndürülemeyecek şekilde tahribi ile mümkündür.[48] Bundan dolayı sayısal deliller, yok edildiği düşünülse de, adli bilişim uzmanları tarafından elde edilebilmektedir. Bir dosyanın silinmesi veya sabit disk sürücüsünün formatlanması durumunda bile sayısal delillerin kurtarılması mümkündür.[49]

Sayısal veriler, çoğu zaman doğrudan delil niteliğine sahip değildirler. Ceza muhakemesine konu olan olay ile ilgisi olduğu halde, çoğu zaman fail, fiil veya mağdur ile aralarındaki ilişkiyi tam olarak yansıtmazlar. Örneğin elektronik posta ile işlenen hakaret suçunda, bilgisayarda bulunan kelime işlemci dosyası, hakaret içeren elektronik postanın öncelikle bilgisayarda taslak olarak hazırlandığı yönünde bir fikir verebilir. Ancak gerçekten bu dosyanın, şüpheli tarafından oluşturulduğunu göstermez. Bu durum, sayısal delillerin delil olma niteliklerini etkilemez, ancak bazen diğer delillerle de desteklenmesini gerektirebilir.[50]

III. SAYISAL DELİLİN DEĞİŞTİRİLEMEZLİĞİNİ SAĞLAMANIN YOLU OLARAK ÖZETLEME

1. Genel olarak

Fiziksel delillerle karşılaştırıldığında kolaylıkla birebir kopyanın çıkarılabilir olması, orijinal veriye ekleme veya çıkarma yapılabilme olanağının olması ve verinin özellikle adli kopyalama aşamasında sehven değiştirilebilme ihtimalinin bulunması, sayısal delilin değiştirilmediğini ortaya koyan matematiksel hesaplamaların yapılmasına adli bilimler dünyasını itmiştir. Bunun sonucu olarak da, özetleme fonksiyonunun kullanılması, sayısal delilin elde edilmesi ve yargılama esnasında mahkemenin hükmüne esas teşkil edebilmesi açısından uygun bir araç olarak ortaya çıkmıştır.

Özetleme (hashing – hash function), kriptografik bir fonksiyon (işlev) olarak, isteğe bağlı uzunluktaki girdiyi (dosya, veri veya bütün bir disk), sabit uzunluktaki bir özet değere eşleştirmektedir. Bu fonksiyonun, amaçlananı gerçekleştirebilmesi için bazı gereklilikleri karşılaması da gereklidir. Bu gereklilikler; a) öncelikle aynı girdinin özet değeri olarak iki farklı

---

44 Casey, 2004, 15.

45 Casey, 2004, 15.

46 Göksu, 32.

47 Casey, 2004, 15; sayısal deliller, bilişim sisteminin içinde depolandığı sürece veya aktarım esnasında tahrif edilebilirler (Sommer, Downloads, 142).

48 Göksu, 32.

49 Casey, 2004, 15.

50 Uzunay, Yusuf – Koçak, Mustafa, "Bilişim Suçları Kapsamında Dijital Deliller", Akademik Bilişim Konferansı Gaziantep, Şubat 2005, 3.

çıktının bulunmaması, b) aynı girdi bakımından iki farklı çıktının bulunmaması ve c) özet değerden hareketle, girdiye ulaşılmasının mümkün olmamasıdır.[51]

2. Sayısal Delilin Değiştirilemezliğini Sağlama Yöntemi Olarak Özetleme

Yukarıda da ifade edildiği üzere sayısal delilin en önemli özelliği kolaylıkla değiştirilebilir, silinebilir, yok edilebilir, kısacası manipüle edilebilir olmasıdır. Casey'in "delil dinamikleri" olarak isimlendirdiği bu husus da, sayısal delilin söz konusu özelliği ile ilgilidir. Sayısal delilin olay yerinden mahkemenin hükmüne esas alındığı ana kadar değiştirilmediğinin delil zinciri (chain of custody) ile garanti altına alınması gereklidir.

Burada yer alan *"değiştirilmeme"* ilkesi, sayısal delilin olay yerindeki veri taşıyıcısından adli kopyalanmasından, bilirkişi incelemesine tabi tutulması anına kadar geçerlidir. Bunun sağlanabilmesi de, ancak birtakım matematiksel hesaplama yöntemleriyle mümkündür.

Delil niteliği göz önünde tutulduğunda verinin bulunduğu araçtan alınması ve analize tabi tutulmasında en önemli ilkelerden birisi, delile ve dolayısıyla da veriye zarar verilmemesidir. Delilin gerek elde edilme gerekse de inceleme aşamasında zarar görmesi, delil üzerinde şüpheyi oluşturacaktır ki, bu durumda delilin tahrif edildiği hususunun ileri sürülmesine neden olacaktır. Bunun önlenmesi için adli bilişim uzmanları her zaman sayısal delilin bir kopyası üzerinde çalışmaktadırlar. Sayısal delilin, birebir kopyasının kolaylıkla çıkartılabilmesi de, bu çalışmayı olanaklı kılmaktadır.

Dolayısıyla öncelikle verinin bulunduğu yerden alınması esnasında yapılan kopyalamanın hatasız olduğunu ve sonrasında ise adli bilişim uzmanının, hatasız kopya üzerinde çalıştığının doğrulanması gerekir. Bu doğrulama özet değer üretilmesi/özetleme (hash value/hashing) ile mümkündür.[52]

Özetleme veya özet değer üretme, bir bilgi dizgesi olan bilgisayar dosyasının (veya herhangi sabit olmayan boyuttaki bir veri dizgesinin), matematiksel işlemlere tabi tutulmak suretiyle, başka bir karakter veya sembole çevirme işlemidir.[53] Tek yönlü özetleme fonksiyonları ile gerçekleştirildiğinde sonlu ve değişken uzunluktaki her bir veriyi sabit uzunluktaki bir çıktıya çevirmek suretiyle yapılmaktadır. Bu işlemin sonucunda girdinin boyutuna bağlı olmaksızın, kullanılan özetleme fonksiyonuna göre benzeri olmayan ve sabit uzunlukta 16'lı sayı sistemine göre A,B,C,D,E,F harfleri ile 0,1,2,3,4,5,6,7,8,9 rakamlarının kombinasyonundan oluşan bir çıktı elde edilmektedir.

Özetleme üç temel esas üzerine inşa edilmektedir. Öncelikle özet değer fonksiyonu, girdinin boyutuna bağlı olmaksızın sayısal veriyi kolaylıkla belirli bir özet değere çevirmelidir. İkinci olarak, özet değerden veriye ulaşılamamalıdır. Ve son olarak ise aynı özet değerine sahip iki farklı bilgi dizgesine rastlanmamalıdır.

Özet değer hesaplamada kullanılan değişik algoritmalar mevcuttur. Söz konusu algoritmalar, özet değerde kullanılan bit sayısına ve üreticisine göre değişik şekillerde isimlendirilmektedirler. Özet değerler, adli kopyanın alınmasında kullanılan yazılım ve donanımın türüne göre sistem tarafından otomatik olarak hesaplanmakta ve bir günlük (log) dosyasında tutulmaktadır.

---

51 Florian Mendel – Norbert Pramstaller – Christian Rechberger – Marcin Kontak – Janusz Szmidt, "Cryptanalysis of the GOST Hash Function", in: *CRYPTO 2008, LNCS 5157* (Ed. D. Wagner), (Springer 2008), 162 (pp. 162 – 178).

52 Tyler Newby –Joel M. **Schwarz**, "Rethinking The Storage of Computer Evidence", UNAFEI Resource Material Series NO. 79, December 2009, Tokyo, 44

53 Stephen **Hoffman**, "An Illustration of Hashing and Its Effect on Illegal File Content in the Digital Age", *Intellectual Property & Technology Law Review*, Vol. 22, No. 4, April 2010, 6; Lily R. **Robinton**, "Courting Chaos: Conflicting Guidance from Courts Highlights The Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence", *Yale Journal of Law and Technology*, Vol. 12, 2010, 326; Danielle **Sutton**, "Computer Forensics and Child Pornography Investigations", *Stevenson Universiy Forensics Journal*, Vol. 2, 2011, s. 31; Michael **Harrington**, "A Methodology for Digital Forensic", *T.M. Cooley J. Parc. & Clinical L.*, Vol. 7, 2004, 73; Marcia **Hoffmann**, "Arguing for Suppression of 'Hash' Evidence", *The Champion*, May 2009, 20, 21.

Özet değerle ilgili olarak bilinmesi gereken husus, özet değer hesaplamasının, bilişim sistemlerinde aramada ilk müdahale esnasında eş zamanlı olarak yapılmasıdır. Verinin yer aldığı sisteme müdahale edildikten sonra veri eklenmesi ve daha sonra özet değerin alınması durumunda, daha sonra alınan özet değerlerde verinin eklendiğinin anlaşılması mümkün değildir. Dolayısıyla arama esnasında gerek adli bilişim uzmanının gerekse de aramaya nezaret eden şüpheli veya müdafi açıdan elzem husus, sistemin öncelikle adli kopyası alınırken nezaret edilerek kopyalama sonucunda oluşan özet değerin arama ve el koyma tutanağına yazılmasıdır.

Aşağıda bazı özet değer algoritmaları ve kullandıkları bit uzunlukları verilmiştir. İfade etmeliyiz ki, algoritmanın sonucu olan özet değer ne kadar uzunsa, daha sonra ifade edileceği üzere özet değeri hesaplanan dosyaların özet değerlerinin çakışma (aynı olma) olasılığı o kadar az olacaktır.

MD-5	SHA-1	SHA-256	SHA-512	RIPEMD-160
128	160	256	512	160

Anlatımlarımızı gerçekleştirdikten sonra bir özet değer uygulaması yapmak uygun olacaktır. Yukarıda da ifade edildiği üzere özet değer hesaplamasında, girdinin boyutu önemli değildir. Bu kapsamda girdi, bütün bir disk, bir disk üzerindeki veriler olabileceği gibi basit bir dosya veya karakterler de olabilir.

İnternet üzerinden kolaylıkla ulaşabileceğiniz bir siteden[54], girmiş olduğumuz ve birbiri ile sadece 1 harf farklığı olan ancak anlam bakımından ciddi farklılıklar bulunan verinin MD5 özet değerleri aşağıda verilmiştir. Buradan da görüleceği üzere 1 harf farklılığında bile çıkan özet değer birinden tamamen farklı olacaktır.

Girilen Veri	**MD5 Özet Değeri**
Aslı'nın katili Erhan'dır.	ed201585e438caf37608948d746e7970
Aslı'nın katili Erkan'dır.	a5cd741fb93893819b96195b5896bb6d

IV. ÖZET DEĞER ÇAKIŞMASI VE SONUÇLARI

Özet değer almak için kullanılan algoritmalarla ilgili geçerlilik ve güvenilirlik tartışması uzun zamandır yapılmakta ve bu konuda literatürde değişik görüşler ifade edilmektedir. Örneğin 32 bitlik uzunluğa sahip olan MD5 özet değeri ile ilgili olarak görüşler ikiye ayrılmaktadır. Birinci görüş taraftarlarına göre MD5 yöntemiyle yapılan özetleme son derece güvenilir sonuçlar vermektedir. Yöntemin, kırılabilmesi ve farklı bit dizgeleri için aynı sonuçların üretilmesi, en azından kontrollü ortamlar hariç olmak üzere mümkün olmadığı ifade edilmektedir. Hatta bazı yazarlar tarafından MD5 özet değerin, en az DNA delili kadar geçerli ve güvenilir sonuçlar verdiği ifade edilmiştir.[55]

Bu konuda ikinci görüş ise özellikle İsrail ve Çin teknoloji üniversitelerindeki çalışmalar sonucu gelişmiş ve birbiri ile çakışan iki özet değerin yaratılabilmesinin mümkün olduğunu ifade etmiştir.[56]

---

54 https://md5.hesaplama.net/hesaplama.do, Erişim Tarihi: 05 Aralık 2017.

55 Warren G. **Kruse** – Jay G. **Heise**, *Computer Forensic: Incident Response Essentials*, 2002, s. 89.

56 Eric **Thompson,** "MD5 Collisions and the Impact on Computer Forensics", *Digital Investigation*, Vol. 2, 2005, 36; Alaeldin Mansour Safauq **Maghaireh**, Jordanian Cybercrime Investigations: A Comparative Analysis of Search for and Seizure of Digital Evidence, Thesis Submitted in Fulfilment of the Requirements for the Award of the Degree, University of Wollonong 2009, 135.

Özet değer çakışmasının olasılığı dikkate alındığında, elde edilen veri üzerine eklemeler yapılarak daha sonra aynı özet değerin üretilebilmesi olanaklı hale gelebilir. Bu da, savunma makamı tarafından maddi olayın ispatı için gerekli olan sayısal verinin güvenilirliğinin olmadığının ileri sürülmesine, yargılama makamı tarafından da söz konusu delilin sahihliği üzerinde şüphe bulunduğundan hükümde kullanılması noktasında tereddüt yaşanmasına neden olacaktır.

Öncelikle çakışma olasılıklarının değerlendirmesini yapmak gerekecektir. Şöyle bir örnekle konuyu izah etmeye çalışalım. CMK 134 kapsamında yapılan bir arama esnasında şüphelinin kullandığı bilgisayarda yer alan bazı verilerin, Cumhuriyet savcılığı tarafından isnat edilen suçun ispatı için yeterli olduğu ve bundan dolayı da önce özet değerinin hesaplandığını, söz konusu özet değer sonucunun savunma makamına verildiğini daha sonra da, adli kopyasının alınarak muhafaza altına alındığını kabul edelim. Daha sonra adli emanette veya bilirkişi incelemesinde söz konusu adli kopyaya bazı eklemeler yapılması ve yeniden özet değer hesaplanması durumunda aynı özet değerin bulunması, özet değer çakışması olarak kabul edilecektir.

Yukarıda yer alan olasılık da, delilin güvenilirliği sarsılacak, gerek savunma gerekse de yargılama makamları tarafından tereddütler yaşanacaktır. O halde, söz konusu çakışma olasılığının ihmal edilebilir olup olmadığına da değinmek gerekecektir. Giriş bölümündeki sözde de ifade edildiği gibi bilimde kesinlik hiçbir zaman yoktur. Dolayısıyla özet değerler bakımından çakışma olasılığının bulunması, uygulanan yöntemin bilimsel olmadığını, adli yanılgılara sebep olduğunu her zaman göstermez. Ortaya konması gereken çakışma olasılığının matematiksel oranıdır. Bu oranı da ortaya koyabilmek için bazı varsayımlardan yola çıkmak zorundayız.

15 Temmuz 2016 sonrasında ülkemizde yapılan yargılamalar bakımından (darbe girişimi yargılamaları ve silahlı terör örgütüne üyelikten dolayı) delil olarak ele geçirilen sayısal materyal için olasılık hesaplaması yaparak konuyu açıklamak istemekteyiz. Bu kapsamda haklarında dava açılan kişi sayısının 100.000 olduğu ve her bir kişi bakımından da 5 adet veri taşıma aracının (mobil telefon, bilgisayar, taşınabilir bellek gibi) incelenmesi gerektiğini düşünelim. Buna göre 500.000 incelemede, aslında farklı bir veri içermesine rağmen aynı özet değerlerin çıkma olasılığı aşağıdaki tabloda verilmiştir.[57]

Algoritma	MD-5	SHA-1	SHA-256	SHA-512	RIPEMD-160
Bit Sayısı	128	160	256	512	160
Çakışma Olasılığı (500.000 materyal içinde)	$3{,}673412 \times 10^{28}$	$8{,}552829 \times 10^{38}$	$1{,}079518 \times 10^{66}$	$9{,}322907 \times 10^{144}$	$8{,}552829 \times 10^{38}$

Bu olasılığa ayrıca şu değeri de ekleyebiliriz. Her bir soruşturmada el konulan cihazlarda, sistem ve kullanıcı dosyası (system and user file) olarak 1.000 dosya bulunduğunu düşünelim. Bu ihtimalde özet değer çakışması olasılığını 500.000.000 girdi arasında hesaplamamız gereklidir.

57 Hesaplamada http://davidjohnstone.net/pages/hash-collision-probability internet sitesi kullanılmıştır ve her bir algoritmanın bit sayısı ve incelenen materyal arasındaki çakışma olasılığı incelenmiştir.

Algoritma	MD-5	SHA-1	SHA-256	SHA-512	RIPEMD-160
Bit Sayısı	128	160	256	512	160
Çakışma Olasılığı (500.000.000 materyal içinde)	3.673419×10^{-22}	8.552847×10^{-32}	1.079521×10^{-60}	9.322925×10^{-138}	8.552847×10^{-32}

Yukarıda verilen olasılıklar şu anlama gelmektedir. 500.000 veri saklama materyalinden alınan, 500.000.000 farklı dosya girdisine ait özet değerlerin, girdi verinin değişmesine rağmen özet değerin aynı olma olasılığı algoritmanın bit sayısına göre artan bir şekilde verilen rakamlardır. Bu hususu şu şekilde de yorumlayabiliriz, bir kişiye ait sayısal materyalde 500.000.000 dosya var ise, iki farklı dosyanın aynı özet değere sahip olma olasılığı da yukarıdaki gibidir.

V. SONUÇ

Buradan çıkartacağımız sonuç, evet özet değerlerin matematiksel formüller olduğundan dolayı iki farklı veri girdisinde aynı özet değerin çıkma olasılığı mevcuttur. Ancak bu olasılıklar, verinin bütünlüğünü sağlayan özet değerlerin kullanılmasını engelleyecek veya delil üzerinde şüphe yaratacak düzeyde değildir.

Ayrıca, kopyası alınan veri depolama aygıtlarının (Sabit disk, USB bellek v.b.) bütününe ait özet değerlerin başka bir soruşturma ya da davadaki kopyası alınan veri depolama aygıtının özet değeri ile aynı olma olasılığı imkansıza yakındır. Şayet aynı özet değere sahip iki veri depolama aygıtı tespit edilirse, bu iki aygıtın da adli bilişim incelemesine tabi tutulması ve özet değerlerinin neden aynı olduğunun açıklanması gerekir. Bugüne kadar yapılan çalışmalarda; özet değerinin bire bir aynı olduğu veri depolama aygıtlarının ya hiç kullanılmamış aynı marka ve model veri depolama aygıtı olduğu ya da bir birinin kopyası (klonu) olduğu bilimsel olarak izah edilmektedir.

Diğer bir husus ise adli kopyalar içerisindeki dosyaların özet değerlerinin aynı olması hususudur. Bu olay hemen hemen her adli kopya içerisindeki dosyalar için geçerlidir, zira işletim sistemlerinin standart dosyalarının özet değerleri aynı olacaktır. Özet değerlerinin aynı olduğu dosyaların içeriğine ve metadata (üstveri) bilgilerini de inceleyip değerlendirmek yine adli bilişim açısından bilinen ve çoğunlukla yapılan bir çalışmadır.

“DARKNET”: KARANLIK AĞDA ARAŞTIRMA - DİJİTAL YER ALTI DÜNYASINDA GİZLİ SORUŞTURMA YAPAN ADLİ KOLLUK GÖREVLİSİ VE GİZLİ SORUŞTURMACI

Dr. Öğr. Üy. Reşit KARAASLAN

Darknet nedir? İnternet, yalnızca arama motorları (örneğin Google, Yahoo) vasıtasıyla ulaşılan ve herkes tarafından görülebilen internet sayfalarından oluşan (surface-web) bir sistem değildir. Buzdağının görünen kısmı olan surface-web’in dışında bir de deep-web olarak isimlendirilen ve Türkçeye derin internet olarak çevrilebilecek bir sistem daha mevcuttur. Derin internet, arama motorları tarafından indekslenmeyen tüm sitelere verilen ortak bir isimdir. Dolayısıyla derin internete, aslında arama motorlarının henüz olmadığı dönemlerde internetin çalışma fonksiyonunu bugün halen devam ettiren bir sistemdir, demek yanlış olmayacaktır. Zira nasıl ki, arama motorlarının olmadığı dönemde internet kullanıcılarının bir internet sayfasına ulaşmak için sayfanın tam adresini adres çubuğuna girmeleri gerekmekteydi, deep-net internet sayfalarına da ulaşmak isteyen internet kullanıcısı hedeflediği sayfanın tam adresini bilmek zorundadır, yoksa söz konusu sayfaya ulaşması mümkün olmayacaktır. Bir internet kullanıcısının deep-web site kurmasının, buraya girmesinin veya benzeri aktiviteleri yapmasının birçok nedeni olabilmektedir. Örneğin şirketlerin gizli kalmasını istedikleri bazı şirket bilgilerini, bilim insanlarının çalışmalarını cloud (bulut) sistemlere duydukları güvensizlik nedeniyle buralarda sakladıkları bilinmektedir. Dolayısıyla derin internet kullanıcılarının her zaman suç işlemek amacında olmadıkları ortadadır.

Ancak internetin suçta araç olarak kullanılması veya suç mahallinin internet olması hiçbir şekilde istisna değildir. İşte derin internetin bir parçası kabul edilen ve karanlık ağ (dark-web ya da darknet) olarak adlandırılan bölümü tam da bu amaçla kullanılan bir sistemdir. Burada suçun hizmet olarak sunulduğu (crime-as-a-service), yasadışı faaliyetlerin gündelik hayat olduğu genel olarak kabul edilmektedir. Bir nevi online yeraltı ekonomisi (underground economy) yaratıldığı bu alanda, silah ve uyuşturucu ticareti; çocuk pornografisi, canlı olarak izlenebilen çocuk istismarı; çeşitli ülkelere ilişkin pasaport, kimlik temini; zararlı yazılım; hassas bilgilerin alım ve satımı; veri hırsızlığı; suç faaliyetleri için kurye ağı sağlamak gibi her türlü illegal hizmet sunulmaktadır. Hatta bu tür hizmetlerden yararlanmak isteyen kullanıcıların, tek tek forumlarda gezinerek arzuladıkları illegal mal veya hizmeti bulmasının zor olması karşısında, aradıklarını daha kolay bulabilmesi, fiyat analizi yapabilmesi ve kendileri

için en uygun tedarikçiyi seçebilmeleri için alıcı ve satıcıyı bir araya getiren "Silk Road", "AlphaBay" ve "Hansa" gibi çeşitli ticari platformların kurulduğu, işletildiği bile bilinmektedir. Bugün bu tür platformlar üzerinden yapılan alış verişin ticaret hacminin milyar dolarlar seviyesinde olduğu kabul edilmektedir.

Darknet neden popüler oldu? Bilindiği üzere surface-web'de internet kullanıcısı, üzerinden geçtiği her sunucuda parmak izlerini bırakmakta, böylece de istenildiğinde sunucu kayıtları üzerinden kimin, hangi siteye ne zaman girdiği ve ne yaptığı geriye doğru takip edilebilmektedir. Darknet ise tam da bu durama karşı geliştirilmiştir. Darknete en bilinen örneği TOR (The Onion Router) olan özel yazılımlarla girilmektedir. TOR yani Türkçe olarak soğan ağı adı verilen bu tarayıcıya sahip kullanıcı darknette dolaşmaya başladığı zaman, sistem bu kişiyi sürekli olarak değişen birden çok bilgisayar üzerinden hedefe yönlendirmektedir. Bunu yaparken de tıpkı bir soğanın katmanlarının birbirinden bağımsız olması gibi, önceki katmanı oluşturan bilgisayar ile bağlantıyı kesmektedir. Sistem ayrıca TOR kullanıcısının hedeflediği bilgisayar ile kendi bilgisayarı arasındaki iletişimi şifreli gerçekleştirmektedir. Bunun sonucunda da ismi sürekli değişen, bilgi alış verişi yapıldıktan sonra sanal dünyada bir daha ortaya çıkmayan, sonu ".onion" ile biten ve "43456atwkfh.onion" gibi herhangi bir anlam ifade etmeyen sayfalar oluşmaktadır. Böylece darknet üzerinden iletişime geçenler ne IP adresi gibi parmak izlerini bırakmakta ne de kiminle iletişime geçtiklerini bilmektedirler. Hatta son yıllarda darknet kullanıcıları ödemeleri de kripto para birimleri ile yapmakta ve böylece sanal dünyanın gerçek dünya ile bağlantısını daha da zayıflatmaktadırlar. Zira bilindiği üzere en popüler kripto para birimi olan Bitcoin sisteminde para, herhangi bir kimsenin kimliğine bağlı olmayan ve istenildiği ölçüde üretilebilen bitcoin cüzdanı üzerinden transfer edilmektedir. Böylece sunucularda parmak izini bırakmayan darknet kullanıcısı, soruşturma organlarının en gözde taktiklerinden biri olan "parayı takip et" metodunu da bertaraf etmektedir.

Darknet ve Koruma Tedbirleri: Darknet aracılığıyla işlenen suçların soruşturulmasında, bilişim sistemleri aracılığıyla işlenen suçların soruşturulmasında klasik yöntem kabul edilen koruma tedbirleri yetersiz kalmaktadır. Gerçekten de bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma işlemi, ister Türk Hukukunda olduğu gibi ayrı bir koruma tedbiri olarak düzenlensin (CMK m. 134) isterse de Alman Hukukunda olduğu gibi genel olarak arama ve elkoymaya ilişkin hükümler çerçevesinde ele alınsın (§ 94 vd. StPO), bu koruma tedbirinin uygulanabilmesi suç şüphesi altındaki kimsenin belirlenmiş, somutlaştırılmış olmasına yani son tahlilde, kullanıcının IP adresinin bulunmuş olmasına bağlıdır. Ancak darknet, tam da parmak izini ortadan kaldırmak için dizayn edilmiştir.

Koruma tedbirlerine ilişkin genel ilkeler olan yasallık, kıyas yasağı, yasal dayanak ilkesi gibi kurallara dikkat edildiği sürece, bilişim teknolojileri kullanılarak uygulanan koruma tedbirleri olan iletişimin tespiti, dinlenmesi ve kayda alınması (CMK m. 135); teknik araçlarla izleme (CMK 140); ülkemizde kabul edilmeyen ancak Federal Almanya'da yakın tarihte yasal zemine kavuşturulan online arama (§ 100b StPO); yine bu ülkede yakın zamanda kabul edilen ve iki kişinin şifrelenmiş iletişimini son cihaza yüklenen bir yazılımla kırmaya ve sonrasında iletişimi dinlenmeye ve kayda almaya izin veren kaynak telekomünikasyon tespiti koruma tedbiri (§ 100a Fıkra 1 Cümle 2, Cümle 3 StPO) gibi tedbirlerin de, son tahlilde darknette yapılan soruşturmalarda etkili olamayacağı aşikârdır; zira tüm bu tedbirler belli bir seviyeye ulaşmış suç şüphesi altında bulunan belli kimselere karşı uygulanabilecek tedbirlerdir. Böylesi kimselerin belirlenemediği durumlarda, bu tedbirlere başvurmak da mümkün değildir.

CMK 134, 135, 140 gibi modern zamanların koruma tedbirlerinin yetersiz kalması sonucu, kolluk çevrimdışı suçlarla mücadele amacıyla yasada yer verilen diğer koruma tedbirlerine yönelmiştir. Ancak adli kolluğun bu şekilde davranması beraberinde başka hukuki tartışmaları getirmiştir. Adli kolluğun sahte (uydurma) bir kimlik (Legende) veya efsane bir isim (Pseudonym) ya da takma-rumuz bir ad (Nickname) ile internette veri toplaması halinde, adli kolluğun genel kurallara tabi sanal gizli soruşturma yapan adli kolluk görevlisi mi yoksa özel yetkilendirme gereken sanal gizli soruşturmacı mı olarak kabul edileceği duraksamalara neden olmuştur. Bu soruyla hem bağlantılı olarak hem de sorudan bağımsız olarak bir konu daha tartışmaları beraberinde getirmiştir. Adli kolluk görevlileri kendilerinin oluşturduğu yeni hesap aracılığıyla soruşturma yapmaktansa; bir şüpheliden daha önce ele geçirilmiş olan, darknet kullanıcılarının tanıdığı ve bu nedenle rahatlıkla işlem yapmaya hazır oldukları var olan hesabı kullanabilirler mi?

Gizli olarak soruşturmaya katılan kişinin hangi sıfata sahip olacağı hususu bilindiği üzere salt akademik bir tartışma değildir. Zira gizli soruşturma yapan adli kolluk görevlisi kavramı kanuni dayanağını, CMK'nın 160 ve 161. maddelerinde bulmaktadır. Buna karşın gizli soruşturmacı kavramı ise CMK m. 139 göz önüne alındığında, çok daha katı ve farklı usul ve esaslara tabi kılınmıştır.

Gizli olarak soruşturmaya katılan kişinin ne zaman gizli soruşturma yapan adli kolluk görevlisi ne zaman ise gizli soruşturmacı olarak kabul edileceğine dair sınır şu şekilde özetlenebilir: Belli bir şüpheliye veya az sayıda şüpheliye temas ederek, sürekli olmayan şekilde, yani bir defa veya ara sıra, kimliğini saklayarak soruşturma yapan kişinin gizli soruşturma yapan adli kolluk görevlisi olduğu kabul edilmektedir. Buna karşın bir kimsenin

gizli soruşturmacı kabul edilebilmesi için, bu kişinin, gizli soruşturma yapan adli kolluk görevlisinden farklı olarak, sadece isim ve adres gibi bilgilere ilişkin değil, aile durumu ve diğer kişisel verileri de kapsayacak şekilde uydurma bir kimliğe sahip olması gerekmektedir. Ayrıca bu uydurma kimliğin gizli olarak soruşturmaya katılan kişiye uzun süreli olarak verilmesi de diğer bir şarttır.

Ne var ki bu açıklamaların olduğu gibi sanal dünyaya aktarılması mümkün değildir ve maalesef doğrudan bu konuyu ele alan herhangi bir yüksek mahkeme kararı da mevcut değildir. Ancak yine de Alman Federal Anayasa Mahkemesi'nin online aramaya ilişkin 2008 yılında verdiği karar, internette yapılan soruşturmalarda dikkat edilmesi gereken hususlara ilişkin önemli ipuçları sağlamaktadır.

Mahkemeye göre internette yer alan kişisel verilere bir temel hak ve özgürlüğe müdahale etmeden ulaşılabilmesinin mümkün olduğu hallerde, örneğin internette bulunan açık kaynaklar, yazışmalar, erişime açık web siteleri ve burada bulunan açık kodlu veriler söz konusu olduğunda, bu veriler soruşturma organları tarafından da herhangi bir koruma tedbirine ilişkin norma başvurulmaksızın genel yetki kuralları çerçevesinde kullanılabilinir. Buna karşın internette yer alan veriler bir temel hak ve özgürlüğe müdahale olmadan elde edilemiyorsa, soruşturma organlarının bu verileri ele geçirmesi ve kullanması ancak meşru bir sebebin varlığını haklı kılan koruma tedbirine ilişkin özel bir normun varlığı halinde mümkün olabilir.

Ayrıca Mahkemeye göre internette kolluk görevlilerinin efsane bir isim ya da takma-rumuz bir ad kullanması, tek başına temel hak ve özgürlüklere bir müdahale olarak değerlendirilmemelidir. Buna karşın dikkatle incelenmesi gereken husus, bu gerçek olmayan isimler aracılığıyla normal şartlar altında ulaşılamayacak hassas bilgilere ulaşılması ve özellikle bu bilgiler sayesinde ceza muhakemesinde yer alan değişik evrelerde gerekli görülen şüphe seviyesinin kabul edilmesi, temellendirilmesidir. İşte bu nokta, soruşturma organlarının sahip olduğu genel yetki ile soruşturma organlarının bir koruma tedbiri çerçevesinde harekete geçmesi için gerekli olan özel yetkinin belirlenmesi aşamasında çok önemlidir.

Cevaplanması gereken soru, tüm bu açıklamaların darknette gizli olarak soruşturmaya katılan kişi için ne anlam ifade ettiğidir.

Bahsedildiği üzere internette herkese açık bulunan verilere veya Facebook, Twitter gibi aslında belli bir şifre ile girilebilen sosyal medya mecralarında, herkese açık olan paylaşımlara ulaşmak için soruşturma makamlarının herhangi bir özel koruma tedbirine başvurmaları gerekmemektedir. Bu bakış açısı olduğu gibi darknete de aktarılabilir. Darknete en bilinen

örneği TOR olan özel yazılımlarla girilmesi, burada bulunan sayfalarda yer alan bilgilerin veyahut forumlarda yer alan açıklamaların herkese açık olmayan veri olarak değerlendirilmesine neden olmayacaktır. Zira TOR-tarayıcısı herkese açık bir browserdır. Keza bir internet sayfasının darknette bulunması ve kişilerin burada gerçek olmayan isimlerle hareket etmesi, henüz daha burada yer alan bilgilerin üçüncü kişilere kapalı olduğu anlamına gelmemektedir.

Dikkatli bir değerlendirmeye tabi tutulması gereken husus ise, soruşturma organlarının ulaşmaya çalıştıkları verilerin, ister surface-web isterse de darknet olsun, kullanıcı veya sayfa işletmecisi tarafından bir giriş kodu ile veya başka bir şekilde saklandığı durumlardır. İşte böylesi durumlarda gizli olarak soruşturmaya katılan kişinin hukuki niteliği ortaya konulmalıdır. Ancak gerek offline gerekse de online alana ilişkin yapılan açıklamalar ışığında hemen fark edilecek ki, bu kişinin her zaman gizli soruşturmacı olması söz konusu değildir. Bu noktadan hareketle herkese açık olmayan bir veriye, gizli olarak soruşturmaya katılan kişi, uydurma bir kimlik ile değil de yalnızca efsane isim veya takma-rumuz ad ile erişim sağlarsa ve örneğin sayfadaki verileri kendi bilgisayarına aktarırsa ya da örneğin forumda yazılanları yalnızca pasif izleyici olarak takip ederse, bu kişinin gizli soruşturma yapan adli kolluk görevlisi olduğu kabul edilebilir. Aynı sonuç adli kolluk görevlisinin bir foruma, bir chat odasına belirtilen şekilde erişim sağladıktan sonra pasif izleyici konumunu aşarak, burada bulunan diğer kişilerle yalnızca o andaki konuyla ilgili olarak aktif bir şekilde iletişime geçmesi hali için de geçerlidir. Zira örneğin forumda konuşulan bir konu ile ilgili olarak, gizli soruşturma yapan kişinin sorduğu soruya yanıt veren kişi için, o anda söz konusu efsane isim veya takma-rumuz adın ardında gerçekte kimin olduğu, önemli değildir. Bu bakış açısı surface-web'de olduğu gibi darknette de geçerlidir.

Buna karşın herkese açık olmayan bir web sitesine ya da foruma girmek için yalnızca efsane isim veya takma-rumuz ad ve kişinin kendi belirlediği şifre yeterli değilse, bunların yanında giriş koduna sahip olabilmek için kişinin telefon numarası, adres, meslek bilgisi, banka kart numarası gibi bilgiler de vermesi gerekmekte ise artık bu durumda adli kolluk görevlisinin hukuki sıfatının belirlenmesi güçleşir. Bu tip durumlarda gerçek olmayan bir kişinin gerçek olmayan bilgilerini adli kolluk görevlisinin kısa ya da uzun bir zaman diliminde ancak son tahlilde yalnızca kendisine verilen görev için mi kullandığı, bu bilgiler sayesinde yalnızca sayfada bulunan, forumda konuşmalara katılan belli bir kişiyle iletişim mi kurduğu; yoksa adli kolluk görevlisine bu bilgilerin uzun süreli mi verildiği, bu bilgiler sayesinde oluşturulan hesap ile herhangi bir zaman diliminde sayısı belli olmayan kişilerle iletişime geçip geçmediği veya

geçebilecek durumda olup olmadığı kıstas kabul edilmelidir. Gizli olarak soruşturmaya katılan kişinin ilk ihtimalde gizli soruşturma yapan adli kolluk görevlisi, ikinci ihtimalde ise gizli soruşturmacı olduğu kabul edilmelidir.

Ancak sanal dünyadaki bu aktivite sonucu, gerçek dünyada buluşma meydana gelirse ne olacaktır? Bir iki defa örneğin alım satımı yapılacak illegal eşya için şüpheli ile buluşan soruşturmaya gizli katılan sanal kişinin durumu, hukuken uyuşturucu madde ticareti konusunda görünüşte satıcı veya alıcı olarak görev yapan kişi ile büyük oranda benzeşmektedir. Dolayısıyla bu kişinin gizli soruşturma yapan adli kolluk görevlisi olduğunun kabulü daha doğru gözükmektedir. Ancak sanal dünyadaki iletişimin gerçek dünyada buluşmaya dönmesi, bu sırada da gizli soruşturma yapan adli kolluk görevlisinin efsane ismine veya takma-rumuz adına yeni bilgiler ekleyerek uydurma bir kimliğin kabulünü zorunlu kılacak şekilde hareket etmesi ve böylece de buluşma amacını aşacak şekilde buluştuğu kişinin gerçek kimliğine ilişkin bilgiler sağlamaya çalışması, diğer sanal kişilerin gerçek kimliklerine ilişkin bilgiler almaya çalışması gibi sınır olaylarda, gizli soruşturmacıdan bahsetmek daha doğru olacaktır.

Tüm bu açıklamalara rağmen, bir husus hakkında daha açıklamalar da bulunmak gereklidir:

Şüpheliye Ait Hesabın Kullanılması Sorunsalı: Dakneti surface-web'den ayıran önemli bir durum söz konusudur. Darknet kullanan kişiler oldukça tedbirli davranmaktadır. Gerçekten de bu kişiler, hem kendi kimliklerinin ve karşısındaki iletişim partnerinin tamamen anonim kalmasını istemekte hem de yakalanmamak için mutlak şekilde yalnızca daha önceden tanıdıkları hesapla alış veriş yapmaktadırlar. Örneğin çocuk pornografisi sitelerinde yeni bir hesabın diğer kullanıcılar tarafından kabul edilmesi için, yeni açılan hesabın siteye uygun içerikler yüklemesi istenmektedir. Bu olmadığı sürece yeni hesap sahibinin takas ortağı bulma şansı neredeyse yok gibidir. Dolayısıyla darknette soruşturmaya gizli olarak katılan adli kolluk görevlisi, bu kişi yukarıda açıklanan kıstaslar çerçevesinde ister gizli soruşturma yapan adli kolluk görevlisi isterse de gizli soruşturmacı olarak sınıflandırılsın, mutlaka darknet kullanıcıları tarafından güvenilir kabul edilen bir hesaba ihtiyaç duymaktadır. Dolayısıyla cevaplanması gereken soru şudur: Darknette soruşturmaya gizli olarak katılan adli kolluk görevlisi böylesi bir hesaba nasıl sahip olacaktır?

Akla gelen ilk ihtimal, soruşturmaya gizli olarak katılan adli kolluk görevlisinin böylesi bir hesabı kendisinin yaratmaya çalışmasıdır. Ancak bu noktada gizli soruşturmacının suç işleyemeyeceğini düzenleyen norma (CMK m. 139/5) dikkat etmek gerekir. Gizli

soruşturmacının dahi suç işlemeyeceği kanunda açıkça düzenlendiğine göre, gizli soruşturma yapan adli kolluk görevlisinin de benzer sınırlamaya tabi olduğu, çoğun yapamadığını az da yapamaz kuralından rahatlıkla anlaşılmaktadır. Ne var ki bu noktada farklı düşünmek mümkündür. Gerçekten de darknette kullanıcıların sorumlu olduğu ağır suçları önlemek amacıyla göreceli olarak daha hafif suç işleyen adli kolluk görevlisinin hukuka uygunluk nedenlerinden ya da en azından kusurluluğu ortadan kaldıran nedenlerden faydalanması mümkün gözükmektedir. Bu noktada gizli soruşturmacının suç işleyemeyeceğini düzenleyen normun öğreti tarafından da mutlak algılanmadığı, örgütün içine girmek için gerekli olan ufak eylemleri işleyebileceği, aksinin kabulü halinde koruma tedbirinin hiçbir zaman başarı sağlamayacağı noktasında görüş bildirdiğinin de unutulmaması gerekir. Bu noktadan hareketle, soruşturmaya gizli olarak katılan adli kolluk görevlisinin örneğin daha önceki bir soruşturmada elde edilen çocuk pornografisi fotoğrafını sisteme yükleyebileceği kabul edilebilir. Buna karşın örneğin bir çocuğun canlı yayında istismarına ilişkin bir videonun ise bu kapsamda değerlendirilmesi pek tabi ki oldukça zordur.

Ancak kabul etmek gerekir ki bu varsayımın her zaman mahkemelerce de kabul edileceğini söylemek oldukça güçtür. İşte tam da bu nedenden dolayı adli kolluk görevlileri, darknette soruşturma yaparken daha önce bir şüpheliden ele geçirilmiş olan, darknet kullanıcılarının tanıdığı ve bu nedenle rahatlıkla işlem yapmaya hazır oldukları hesabı kullanmak istemektedir. Ne var ki bu ihtimalde de tartışılması gereken bazı noktalar mevcuttur. Zira bir şüphelinin sahip olduğu darknet hesabı ceza muhakemesine göre bir delildir; ancak bir delili aramak, bulmak ve ona elkoymak ve daha sonra da delil olan bu hesaptaki hareketleri incelemek, değerlendirmek ve bu hesapla daha önce iletişime geçen diğer hesaplara ulaşmak mümkün ise de; elde edilen darknet hesabı üzerinden daha önceki iletişim partnerleri ile iletişime devam etmek veya yeni muhtemel partnerlerle iletişime geçmek, ne CMK m. 160, 161 ne CMK m. 139 ne de arama ve elkoymaya ilişkin normlar çerçevesinde mümkündür. Dolayısıyla bir şüpheliye ait ele geçirilmiş hesabı kullanmak, kanunda özel olarak düzenlenmelidir. Tam da bu düşüncelerle Federal Almanya'da, Ceza Usul Kanunu'na yeni bir paragraf eklenmesi önerilmiştir. Bu öneriye göre belirli suçlar ile mücadelede, savcılık ve kolluk, darknet sisteminin şüpheliye sunmuş olduğu hesap aracılığıyla üçüncü kişilerle iletişime geçmeye yetkili kılınmaktadır. Hatta teklife göre şüpheli söz konusu hesabın giriş kodlarını vermeye mecbur kılınmıştır.

Sonuç yerine: Gizli olarak soruşturmaya katılan sanal kişinin, hangi durumda sanal gizli soruşturma yapan adli kolluk görevlisi hangi durumda ise sanal gizli soruşturmacı olduğu, her ne kadar offline alanda ortaya konan kıstaslar çerçevesinde ve de sanal dünyaya ilişkin yüksek mahkemelerce ortaya konan ilkeler çerçevesinde bir ölçüde aydınlatılabilmekte ise de, tüm açıklamaların son tahlilde muğlak kaldığı bir gerçektir. Bireylerin temel hak ve özgürlüklerine müdahale olan koruma tedbirlerinin koşullarının ise, yasallık ilkesi çerçevesinde kanunlarda açık ve net olarak ortaya konması bir hukuk devletinde olmazsa olmazdır. Dolayısıyla offline alan düşünülerek kaleme alınan koruma tedbirleri üzerinde, sanal dünyanın gerçeklerini göz ardı etmeden yeniden düşünmekte fayda vardır. Buna, sanal dünya söz konusu olduğunda her ne kadar dillendirilmese de gerçekte sıklıkla başvurulan, kolluk görevlilerinin kendi kimliklerini saklamak suretiyle yaptıkları soruşturmalardan başlamak uygun olacaktır. CMK m. 160, 161 ve CMK m. 139 arasındaki sınırın sanal dünyada ortaya konulmasının neredeyse imkânsız olduğu düşünüldüğünde, bu hükümlerin sanal dünyaya ilişkin tek bir hükümde eritilmesi, oldukça makul bir çözüm önerisi olarak gözükmektedir. Bu yapılırken de şüpheliden elde edilmiş, var olan hesap üstünden kolluk görevlilerinin hangi şartlar altında üçüncü kişilerle iletişime geçebileceği sorusu da unutulmamalıdır. Sınırları açık ve net bir biçimde çizilmiş bir koruma tedbiri unutulmamalıdır ki, bir taraftan toplumdaki herkesin ve de şüpheli ve sanığın temel hak ve özgürlüklerinin korunmasına yardım edecektir diğer taraftan da suç ile mücadelede soruşturma organlarının elini güçlendirecektir.

Özel Hayatın Gizliliği Nedeniyle İnternet Ortamında Yapılan Yayın İçeriğine Erişimin Engellenmesi*

Dr. Öğr. Üyesi Kerim ÇAKIR

Özet: Günümüzdeki bilgi ve iletişim teknolojisi ile internet hayatın her alanına girmiş, bu sayede hak ve özgürlüklerin, özellikle de ifade özgürlüğünün, alanı sanal dünyada epey genişlemiştir. Ancak bu durum beraberinde bireyin özel hayatına ve hayatın gizli alanına müdahaleyi de kolaylaştırmıştır. İnternet ortamında sayısı belli olmayan kişilere ulaşan yayının içeriği, telafisi mümkün olamayacak mağduriyetlere neden olabilir. Bunu dikkate alan kanun koyucu, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 9/A maddesinde, özel hayatı ihlal eden içeriklerin engellenmesi tedbirine yer vermiştir. Bu tedbir, niteliği itibariyle bir koruma tedbiridir. Tedbire müracaat için özel hayatının gizliliğinin ihlal edildiğini iddia eden kişinin Bilgi Teknolojileri ve İletişim Kurumu'na başvurması gerekmektedir. Kuruma yapılan müracaatta hakkın ihlaline neden olan yayının tam adresi, hangi açılardan hakkın ihlal edildiğine ilişkin açıklama ve başvuranın kimlik bilgilerini ispatlayacak bilgilere yer verilir. Daha sonra özel hayatın gizliliğinin ihlal edildiğinden bahisle erişimin engellenmesi talebi sulh ceza hâkimine sunulur. Hâkim, yayın içeriğinin özel hayatın gizliliğini ihlal edip etmediğini değerlendirir.

Prevention of Access to The Publication Content of The Internet Environment for The Privacy of Private Life

Abstract: With the current information and communication technology, the internet has entered every aspect of life, and so the area of rights and freedoms, in particular freedom of expression, has expanded considerably in the virtual world. However, this situation facilitated the intervention of the private life of the individual and the hidden area of life. The content of the publication, which reaches to the persons whose number is not clear on the Internet, may cause grievances that cannot be compensated. Considering this, the legislator, in Article 9/A of Law No. 5651 on the Regulation of Publications on the Internet and the Fight Against Crimes Committed by These Publications, has included measures to prevent the violation of private

* Dr. Öğr. Üyesi Kerim ÇAKIR, Marmara Üni. Hukuk Fakültesi Ceza ve Ceza Usul Hukuku Öğretim Üyesi.

life. This measure is, in its nature, a protection measure. The person who claims that his privacy has been violated for application to the measure should apply to the Information and Communication Technologies Authority. In the application made to the Authority, the full address of the publication causing the violation of the right and the information about the violation of the right and the information to prove the identity shall be included. Then, the demand for the prevention of access, as the privacy of the private life is violated, is submitted to the magistrates. The judge assesses whether the content of the publication violates the privacy of private life.

I. Giriş

Hukuk devletinde fertlere, maddi ve manevi varlıklarını istedikleri gibi geliştirip şekillendirebilecekleri hür bir *"hayat alanı"* tanınır. Devletin müdahalesinden korunmuş bulunan ve *"bireyin küçük dünyası"* olarak anılabilecek bu alan, temel hak ve hürriyetler ile ülkenin siyasi rejimi bakımından hassas bir göstergedir. Bu küçük dünyamız ne kadar geniş ise, ülkede mevcut olan siyasi rejim o kadar hürriyetçi ve demokratik; ne kadar dar ise, o kadar baskıcı ve otoriterdir[1].

1982 Anayasası'nın 20 nci maddesinde, İnsan Hakları Evrensel Beyannamesinin 12 nci maddesinde[2], Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesinin 17 nci maddesinde[3], ve İnsan Hakları Avrupa Sözleşmesinin 8 inci maddesinde[4], fertlerin devletin müdahalelerinden korunmuş hür bir alana sahip bulundukları açıkça ifade edilmiştir.

Anayasamızın; *"temel haklar ve ödevleri"* düzenleyen ikinci kısmının ikinci bölümünün (kişinin hakları ve ödevleri) IV No'lu başlığında; *"özel hayatın gizliliği ve korunması"* düzenlenmiştir.

---

[1] Bkz; Ergun Özbudun, *Anayasa Hukuku Bakımından Özel Haberleşmenin Gizliliği*, (AÜHFD, 50. Yıl Armağanı, C.l Ankara 1977), 265-296; Ahmet Danışman, *Ceza Hukuku Açısından Özel Hayatın Korunması,* (Konya 1991), l vd.; Öztekin Tosun, *Özel Hayatın Gizliliğini İhlal Suçları,* Değişen Toplum ve Ceza Hukuku Karşısında TCK'nın 50 yılı ve Geleceği, (İstanbul 1977), 371 vd.; Ersan Şen, *Gizli Dinleme ve Görüntüleme Fiililerinin Türk Hukuku'ndaki Yeri Üzerine Bir İnceleme,* (İstanbul Barosu Dergisi, C.68, S, 7-8-9, 1993), 502 vd.

[2] İHEB madde 12; *"Hiç kimse, özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfi karışmalara şeref ve şöhretine karşı tecavüzlere maruz kalamaz. Herkesin bu karışma ve tecavüzlere karşı kanun ile korunmağa hakkı vardır"* şeklindedir.

[3] Sözleşmenin 17. maddesinde, *"Hiç kimsenin özel hayatı, ailesi konutu ya da haberleşmesine keyfi ya da yasadışı saldırıda bulunulamaz, herkes, bu tür karışmalara ya da saldırılara karşı kanun tarafından korunma hakkına sahiptir"* denilerek özel hayatın gizliliği güvence altına alınmıştır.

[4] Anayasamızın 90. maddesinin son fıkrasına göre, bir iç hukuk kuralı olan insan Hakları Avrupa Sözleşmesi'nin 8. maddesi şöyledir: *"Her şahıs hususi ve ailevi hayatına, meskenine ve "muhaberatına" hürmet edilmesi hakkına maliktir. Bu hakların kullanılmasına resmi bir makamın müdahalesi demokratik bir cemiyette, ancak millî güvenlik, amme emniyeti, memleketin iktisadi refahı, nizamın muhafazası, suçların önlenmesi, sağlığın veya ahlâkın ve başkasının hak ve hürriyetlerinin korunması için zaruri bulunduğu derecede ve kanunla derpiş edilmesi şartıyla vuku bulabilir."* Sözleşme metni için bkz; Kayıhan ***İçel-Feridun Yenisey,*** *Karşılaştırmalı ve Uygulamalı Ceza Kanunları,* (İstanbul 1989), 57.

Buna göre, herkes özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz (m. 20)[5]. Doktrinde, insanın sosyal bir varlık olduğu ve bu nedenle hayatını ancak diğer insanlarla birlikte devam ettirebileceği gerçeğinden hareketle, insan hayatının, esas itibariyle iki yönünün bulunduğu kabul edilir. Bunlar hayatın genel ve özel yönleridir; hayatın özel yönü de "*özel hayat"* ve *"hayatın gizli alanı"* olmak üzere ikiye ayrılır[6].

Hayatın özel yanı her hukuk devletinde koruma altına alınmıştır. Özel hayat, hayatın gizli alanına dahil olmayan, sınırlı sayıda kişiyle paylaşılan durum ve olayları ihtiva eden hayat alanıdır. İnsan yaratılışı gereği, kendisi ile ilişkili olsun veya olmasın bazı faaliyetlerini üçüncü kimselerden saklama ihtiyacı hisseder. Böylece kişi kendini güvende ve özgür hisseder. Burada kişilerin özel hayatlarına makul saygı beklentisi de bulunmaktadır. Başkalarının bilmediği ve bilmesi gerekmediği, kişinin herkesten gizlediği özel hayatı bu beklentiyi haklı kılmaktadır[7]. Belirtelim ki, özel hayat sosyal yaşamın her alanında vardır. Kişi, konutunda olduğu kadar sokakta da özel hayatına saygılı olunmasını bekleme hakkına sahiptir. Örneğin, eşiyle veya sevgilisiyle birlikte iken mahrem olan fotoğrafları veya videoları sosyal medya üzerinden yayınlanan kişinin özel hayatının gizliliği ihlal ediliyor demektir.

Hayatın gizli alanı ise sadece ferdi ilgilendirir ve ondan başkasının bu alana girebilmesi asla kabul edilemez; bu sebeple de dokunulmazdır[8].

---

[5] Madde Gerekçesi'nde; *"Bu madde ile kişinin özel hayatı korunmaktadır. Kişinin özel hayatı, ferdî, özel hayat ve ayrı bir kavram ve bir "bütün" teşkil eden aile hayatından oluştuğu için her ikisi birlikte ifade edilmiştir. Bu anlamda özel hayatın korunması her şeyden önce bu hayatın gizliliğinin korunması, başkalarının, gözleri önüne serilememesi demektir. Bu cümleden olarak meselâ basın hürriyeti sınırlanabilecek yani, kişinin özel hayatı gazete sayfalarında hikaye edilemeyecektir. Söz konusu gizliliğin korunması, ikinci olarak, kişinin üstünün, özel kâğıtlarının ve eşyasının aranmaması ile sağlanacaktır. (....) Özel hayatın korunmasının diğer bir yönü de resmî makamların özel hayata müdahale edememesi; yani kişinin ferdî ve aile hayatını kendi anladığı gibi düzenleyip yaşayabilmesidir"* denilmektedir.

[6] Hayatın genel ve özel yanlarının birbirinden nasıl ayrılacağı ve özel hayat ile hayatın gizli alanının yekdiğerinden ayırt edilmesi konusunda Alman Anayasa Mahkemesi tarafından "kuşak teorisi = Sphaerentheorie" geliştirilmiştir. Buna göre, insan hayatının merkezinde her türlü devlet müdahalesine karşı korunmuş bulunan ve dokunulmaz olduğu kabul edilen bir çekirdek alan vardır. Bu çekirdek alan, ikinci bir kuşak alanla çevrilmiştir. Bu ikinci alan da devletin müdahalesine karşı korunmuştur. Ancak dokunulmaz değildir. Yani bu alan bakımından nisbî bir koruma söz konusudur. Nihayet insan hayatı bakımından bu ikinci alanı çevreleyen üçüncü bir kuşak alan daha vardır ki, burada herhangi bir koruma söz konusu değildir. Bkz; ***Şen,*** *Gizli Dinleme ve Görüntüleme Fiililerinin Türk Hukuku'ndaki Yeri Üzerine Bir İnceleme,* 504 vd.; Veli Özer Özbek, Koray Doğan, Pınar Bacaksız, İlker Tepe, *Ceza Muhakemesi Hukuku,* (9. Baskı, Ankara 2017), 57, 58.

[7] Hamide Zafer, *Özel Hayatın ve Hayatın Gizli Alanının Ceza Hukukuyla Korunması, TCK m. 132-134*, (1. Baskı, İstanbul 2010), 4; Doğan Kılınç, 5651 *Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 9/A Maddesi Çerçevesinde Özel Hayatın Korunması*, (Gazi Üniversitesi Hukuk Fakültesi Dergisi C. XX, Y. 2016, Sa. 2), 587.

[8] Anayasa Mahkememiz 1967 yılında verdiği bir kararında ilkeyi şu şekilde açıklamıştır: *"Özel hayatın dokunulmazlığı ilkesi, bir kişinin bedeninin tamamlığına dokunmama, var olan özgürlüğünü engellememek kuralı yanında, o kişinin maddi ve manevi alanda sürüp gitmesi demek olan özel hayat ve aile hayatının dokunulmazlığını anlatır. Kişinin mal durumu da özel hayatındandır. Bunun da gizliliğine dokunulmaması gerekir. Fakat her temel hak gibi bu temel hak da Anayasanın 11. maddesi uyarınca özüne dokunmamak koşulu ile kamu yararı ve kamu düzeni gereği yasa ile sınırlanabilir." Bkz; 27.9.1967 tarih ve 1963/336 E., 1067/29 sayılı ilam. 1967/29; R.G.19.10.1968 tarihli nüsha.*

II. Özel Hayatın Gizliliğini İhlal Suçu

Günümüzde bilgiye çok kolay erişilmesi ve bilginin kolayca depolanması insanın faaliyetlerini ve özellikle özel hayatı ile ilgili hususları gizleyebilmesini zorlaştırmıştır. Bu durumu dikkate alan kanun koyucu iletişim araçlarının sağladığı imkânların kötüye kullanılmasına engel olmak amacıyla Türk Ceza Kanunu'nda bireyin özel hayatını koruma amaçlı düzenlemelere yer vermiştir (TCK m. 132-138).

İnceleme konumuz olan özel hayatın gizliliğini ihlal suçu, TCK'nın 134 üncü maddesinde düzenlenmiştir. Madde; *"(1) Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır. (2) Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur"* şeklindedir.

Madde ile gizli yaşam alanına girilerek veya başka suretle başkaları tarafından görülmesi mümkün olmayan bir özel yaşam olayının saptanması ve kaydedilmesi cezalandırılmaktadır. Elde edilen saptama ve kayıtlardan herhangi bir suretle yarar sağlanması veya bunların başkalarına verilmesi veya diğer kimselerin bilgi edinmelerinin temini veya basın ve yayın yoluyla açıklanması suçun ağırlaşmış şeklini oluşturmaktadır.

Maddenin ikinci fıkrasında, kişinin özel hayatına ilişkin görüntü veya seslerin hukuka aykırı olarak ifşa edilmesi, ayrı bir suç olarak tanımlanmıştır. Bu görüntü veya sesler, örneğin soruşturma kapsamında hukuka uygun bir şekilde kayda alınmış olabileceği gibi, birinci fıkrada tanımlanan suçun işlenmesi suretiyle de elde edilmiş olabilir. İkinci fıkrada tanımlanan suç, elde edilmiş olan bu ses veya görüntü kayıtlarının ifşasıyla, yayılmasıyla, yani yetkisiz kişilerce öğrenilmesinin sağlanmasıyla oluşur. Bu ifşanın hukuka aykırı olması gerekir. Bu bakımdan özel hayata ilişkin kayıtların, savcılık veya mahkemeye verilmesi, duruşmada gösterilmesi ve dinlenmesi halinde, söz konusu suç oluşmayacaktır. İfşanın, basın ve yayın yoluyla yapılması, söz konusu suçun nitelikli unsuru olarak kabul edilmiştir.

III. Özel Hayatın Gizliliğinin İhlali Nedeniyle İçeriğe Erişimin Engellenmesi Tedbiri

Özel hayatın özellikle internet aracılığıyla sık ve kolay ihlal edilmesi kanun koyucuyu bireyin özel hayatını koruma adına etkin önlemler almaya mecbur bırakmıştır. Bu kapsamda *"Özel hayatın gizliliğinin ihlali nedeniyle içeriğe erişimin engellenmesi tedbiri"*, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla

Mücadele Edilmesi Hakkında Kanun'a (06.02.2014 tarih ve 6518 sayılı Kanunla) 9/A maddesi eklenmiştir[9].

Bahse konu tedbire müracaat için madde metninde geçen teknik kavramların ne anlama geldiğini bilmek gerekmektedir. 5651 sayılı Kanun'un *"Tanımlar"* başlıklı 2 nci maddesine göre; Bu Kanun'un uygulamasında geçen kavramlardan; "*c) Başkan:* Bilgi Teknolojileri ve İletişim Kurumu Başkanını, *ç) Bilgi:* Verilerin anlam kazanmış biçimini, *d) Erişim:* Bir internet ortamına bağlanarak kullanım olanağı kazanılmasını, *e) Erişim sağlayıcı:* Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri, *f) İçerik sağlayıcı:* İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri, *g) İnternet ortamı:* Haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortamı, *ğ) İnternet ortamında yapılan yayın:* İnternet ortamında yer alan ve içeriğine belirsiz sayıda kişilerin ulaşabileceği verileri, *h) İzleme:* İnternet ortamındaki verilere etki etmeksizin bilgi ve verilerin takip edilmesini, *ı) Kurum:* Bilgi Teknolojileri ve İletişim Kurumunu, *l) Yayın:* İnternet ortamında yapılan yayını, *m) Yer sağlayıcı:* Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri, *n) Birlik:* Erişim Sağlayıcıları Birliğini, *o) Erişimin engellenmesi:* Alan adından erişimin engellenmesi, IP adresinden erişimin engellenmesi, içeriğe (URL) erişimin engellenmesi ve benzeri yöntemler kullanılarak erişimin engellenmesini, *ö) İçeriğin yayından çıkarılması:* İçerik veya yer sağlayıcılar tarafından içeriğin sunuculardan veya barındırılan içerikten çıkarılmasını, *p) URL adresi:* İlgili içeriğin internette bulunduğu tam internet adresini" ifade eder.

---

[9] *"Özel hayatın gizliliği nedeniyle içeriğe erişimin engellenmesi"* başlıklı 9/A maddesinde; *"(1) İnternet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiğini iddia eden kişiler, Kuruma doğrudan başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını isteyebilir. (2) Yapılan bu istekte; hakkın ihlaline neden olan yayının tam adresi (URL), hangi açılardan hakkın ihlal edildiğine ilişkin açıklama ve kimlik bilgilerini ispatlayacak bilgilere yer verilir. Bu bilgilerde eksiklik olması hâlinde talep işleme konulmaz. (3) Başkan, kendisine gelen bu talebi uygulanmak üzere derhâl Birliğe bildirir, erişim sağlayıcılar bu tedbir talebini derhâl, en geç dört saat içinde yerine getirir. (4) Erişimin engellenmesi, özel hayatın gizliliğini ihlal eden yayın, kısım, bölüm, resim, video ile ilgili olarak (URL şeklinde) içeriğe erişimin engellenmesi yoluyla uygulanır. (5) Erişimin engellenmesini talep eden kişiler, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edildiğinden bahisle erişimin engellenmesi talebini talepte bulunduğu saatten itibaren yirmi dört saat içinde sulh ceza hâkiminin kararına sunar. Hâkim, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edilip edilmediğini değerlendirerek vereceği kararını en geç kırk sekiz saat içinde açıklar ve doğrudan Kuruma gönderir; aksi hâlde, erişimin engellenmesi tedbiri kendiliğinden kalkar. (6) Hâkim tarafından verilen bu karara karşı Başkan tarafından 5271 sayılı Kanun hükümlerine göre itiraz yoluna gidilebilir. (7) Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır. (8) Özel hayatın gizliliğinin ihlaline bağlı olarak gecikmesinde sakınca bulunan hâllerde doğrudan Başkanın emri üzerine erişimin engellenmesi Kurum tarafından yapılır. (9) Bu maddenin sekizinci fıkrası kapsamında Başkan tarafından verilen erişimin engellenmesi kararı, (...) yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar"* denilmektedir.

Özel hayatın gizliliğinin internet aracılığıyla ihlal edilmesi halinde ivedi önlemler alınması ve yayına erişimin engellenmesi gerekmektedir. Öncelikle en fazla ihlalin yaşandığı sosyal ağlara *(facebook, twitter, instagram veya youtube gibi)* müracaat etmek gerekir. Bu ağlar, kullanıcıların talep ve şikayetlerini işleme alarak erişimi engelleyebilir. Mümkün olmadığı takdirde 5651 sayılı Kanun hükümleri uyarınca harekete geçmek gerekir.

5651 sayılı Kanun'un 9/A maddesinde yer alan özel hayatın gizliliğinin ihlali nedeniyle içeriğe erişimin engellenmesi, niteliği itibariyle bir koruma tedbiridir. Ceza muhakemesinin yapılmasını veya yapılan muhakemenin sonunda verilecek kararların yerine getirilebilmesini sağlamak amacıyla kural olarak, ceza muhakemesinde karar verme yetkisine sahip olanlar tarafından geçici olarak başvurulan ve muhatabının temel hak ve hürriyetlerine müdahaleyi gerektiren kanuni çarelere *"koruma tedbiri"* denir[10].

Koruma tedbirleri esasında tali ceza davası niteliğindedir. Bunların uygulanabilmesi için talep üzerine ceza muhakemesinde karar vermeye yetkili olan makamlar tarafından işlem yapılması, yani tali ceza davası açılması gerekir.

Bahse konu tedbire müracaatın usulü de maddede gösterilmiştir. Buna göre, internet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiğini iddia eden kişiler, Kuruma doğrudan başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını isteyebilir (m. 9/A-1). Talep bulunmadıkça, re'sen böyle bir tedbir kararı alınması mümkün değildir.

Yapılan bu istekte; hakkın ihlaline neden olan yayının tam adresi (URL), hangi açılardan hakkın ihlal edildiğine ilişkin açıklama ve kimlik bilgilerini ispatlayacak bilgilere yer verilir. Bu bilgilerde eksiklik olması halinde talep işleme konulmaz. Başkan, kendisine gelen bu talebi uygulanmak üzere derhal birliğe bildirir, erişim sağlayıcılar bu tedbir talebini derhâl, en geç dört saat içinde yerine getirir (m. 9/A-2, 3).

Erişimin engellenmesi, özel hayatın gizliliğini ihlal eden yayın, kısım, bölüm, resim, video ile ilgili olarak (URL şeklinde) içeriğe erişimin engellenmesi yoluyla uygulanır (m. 9/A-4).

Erişimin engellenmesini talep eden kişiler, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edildiğinden bahisle erişimin engellenmesi talebini, talepte bulunduğu saatten itibaren yirmi dört saat içinde sulh ceza hâkiminin kararına sunar.

---

[10] Ahmet Gökcen, Murat Balcı, Mehmet Emin Alşahin, Kerim Çakır, *Ceza Muhakemesi Hukuku,* (3. Baskı, Ankara 2018) 356, 357.

Hâkim, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edilip edilmediğini değerlendirerek kararını en geç kırk sekiz saat içinde açıklar ve doğrudan Kuruma gönderir; aksi hâlde, erişimin engellenmesi tedbiri kendiliğinden kalkar (m. 9/A-5).

Hâkim tarafından verilen bu karara karşı Başkan tarafından 5271 sayılı Kanun hükümlerine göre itiraz yoluna gidilebilir. Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır (m. 9/A-7). Yayından çıkarılan içeriğin denetimini başvurucu kendisi yapabilir[11].

Özel hayatın gizliliğinin ihlaline bağlı olarak gecikmesinde sakınca bulunan hâllerde doğrudan Başkanın emri üzerine erişimin engellenmesi Kurum tarafından yapılır (m. 9/A-8). Başkan tarafından verilen erişimin engellenmesi kararı, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar (m. 9/A-9).

Belirtelim ki, tedbirin uygulanması için maddede herhangi bir şüphe derecesinden bahsedilmemiştir. Bu sebeple ceza muhakemesinin temel prensipleri dikkate alınarak değerlendirme yapmak gerekir. Düşüncemize göre, özel hayatın gizliliğinin ihlali nedeniyle içeriğe erişimin engellenmesi için özel hayatın gizliliğinin ihlal edildiğine dair "yeterli suç şüphesi"nin varlığı aranmalıdır. Madde metninde suç şüphesinden bahsedilmese de başlangıç ve makul şüphe ile tedbire müracaatın zorluğu dikkate alındığında yeterli suç şüphesinin tespiti yayın içeriğinin engellenmesini gerekli kılacaktır.

Basın hürriyeti, haber verme ve haber alma hakkı dikkate alındığında bu koruma tedbirine müracaat için basit veya makul şüphe yeterli olmaz, basının haber verme hakkının korunması bakımından burada en azından *"yeterli şüphe"*nin bulunması gerekir.

Özel hayatın gizliliğinin ihlali halinde sadece ihlale konu yayın, kısım, bölüm, resim veya videoya erişim engelleme tedbiri uygulanabilir. Özel hayatın gizliliğinin ihlal edildiğinden bahisle sitenin tamamına erişim engelleme kararı verilemez. İhlale neden olan içerik nedeniyle sitenin tamamına erişimin engellenmesi, ölçülülük ilkesine aykırı olacaktır[12].

Sitenin tamamı için erişim engelleme kararı, 5651 sayılı Kanun'un 9 uncu maddesine göre kişilik hakkı ihlali kapsamında ve ihlalin bertaraf edilebilmesi için zorunluluk arz etmesi durumunda verilebilir[13].

---

[11] Kılınç, *5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 9/A Maddesi Çerçevesinde Özel Hayatın Korunması*, 603.
[12] Kılınç, *5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 9/A Maddesi Çerçevesinde Özel Hayatın Korunması*, 602.
[13] Murat Tumay, *Denetim ve Özgürlük İkileminde İnternet Erişimi,* (Temmuz 2015), 15.

İnternet ortamında yapılan yayının haber olduğu konusunda kamu yararı olduğunun düşünülmesine rağmen, haberin içerik biçimlendirmesi ve sunuluş şeklinin kamuoyu nezdinde isnat edilen eylemi kesin olarak işlemiş bulunduğu intibaı yaratmak suretiyle ölçüsüz uygulamalar masumiyet karinesine zarar vermektedir. Yapılan yayınlarda kişinin isminin tamamının ya da baş harfinin veya çalıştığı yerin ya da ailesi ile bilgilerin açıkça yer alması mağduriyetlere neden olabilmektedir.

Özel hayatın gizliliğinin ihlali nedeniyle yapılan başvurularda önemli olan bir diğer husus, gerek idari gerekse de adli mercilerin kişilerin hukuki korunma taleplerini gerekçe göstermeksizin reddetmesidir. Anayasa Mahkemesi'nin 19.11.2014 tarih ve 2013/5895 sayılı kararında; *"başvurucu hakkında başvuruya konu olay nedeniyle kamu davası açılmış olduğu, yargılamanın aleni olduğu ve basın özgürlüğü kapsamında konunun ilgili basın yayın kuruluşlarınca yorum katılmaksızın haber yapıldığı, haberin yanlış çıkması durumunda dahi hak ihlali kastı ile hareket etmeyen gazetecinin bundan sorumlu tutulmayacağı belirtilerek ve başvuruya konu yayın içeriğine dair somut tespit ve değerlendirmede bulunulmaksızın tekzip talebinin reddedilmesi, (...) başvurucunun yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğine ilişkin temel iddialarının değerlendirilerek karşılanmadığı anlaşılmaktadır. Açıklanan nedenlerle, başvurucunun Anayasa'nın 36. maddesinde güvence altına alınan gerekçeli karar hakkının ihlal edildiğine karar verilmesi gerekir"* denilmek suretiyle bu husus vurgulanmıştır.

BİLİŞİM SİSTEMİNE GİRME SUÇUNDA İÇTİMA

Araş. Gör. Büşra ÖZÇELİK•

ÖZET

Bilişim sistemine girme suçu başta bilişim sisteminin güvenliği ve güvenilirliği olmak üzere kişisel veriler, kişilerin özel hayatı, ticari hayat, ulusal ve uluslararası güvenlik gibi pek çok hususu tehdit edebilecek nitelikte olan ve bilişim suçlarının da çekirdeğini oluşturan temel bir bilişim suçudur. Bu bakımdan 5237 sayılı TCK'nın 243'üncü maddesinde yer alan bilişim sistemine girme suçunda içtima hususunun incelenmesi ihtiyacı doğmuştur. Bu bağlamda zincirleme suç hususundaki gündeme gelebilecek sorun ve sorunsallara yer verilecektir. Ardından fikri içtima bakımından bilişim sistemine girme suçu değerlendirilecektir. Söz konusu suç tipinin icra hareketlerinin başkaca suç tiplerinin icra hareketleriyle tamamen veya kısmen örtüşmesi muhtemeldir. Bu sebeple bu çalışmada bilişim sistemine girme suçu ile başkaca suçların aynı anda gündeme geldiği hallerde farklı neviden fikri içtimaın mı yoksa görünüşte içtimaın mı uygulanacağı hususunun tartışılacaktır.

ABSTRACT

The crime of unauthorized access to information system is a fundemental cybercrime that can threaten many areas such as personal data, personal life, commercial life, national and international security and especially the security and reliability of the information system. Therefore, there is a crucial need to examine the issue of concurrence in unauthorized access to information system regulated in article 243 of the Turkish Penal Code No. 5237. In this context, problems that may arise on the issue of successive offence will be examined. Then the crime of unauthorized access in terms of conceptual aggregation will be evaluated. It is possible that the enforcement actions of this type of crime will fully or partially overlap with the enforcement actions of other types of crime. For this reason, it will be discussed whether joinder of crimes or unreal joinder of crimes will be applied in cases where the crime of unauthorized access to information system and other crimes are brought up at the same time.

• İstanbul Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı.

A. Genel Olarak

Bilişim sistemine girme suçu 5237 sayılı TCK'nın 243'üncü maddesinde yer almaktadır. Anılan madde şu şekildedir:

"*Bilişim sistemine girme*

Madde 243- (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur."

Doktrinde, bilişim sistemine girme suçunu düzenleyen 243'üncü maddenin 2'nci ve 3'üncü fıkrasının aynı anda gündeme geldiği hallerde nasıl bir yol izlenmesi gerektiği tartışılmıştır. TCK'nın 243'üncü maddesi kapsamında failin bedeli karşılığı yararlanılabilen bir sisteme girip taksirli hareketi neticesinde bu sistemde yer alan verilerin yok olması veya değişmesi halinde failin cezai sorumluluğunun nasıl belirlenmesi gerektiği konusunda iki yaklaşım ortaya konulmaktadır. İlk yaklaşıma göre 243'üncü maddenin 2'nci fıkrasında yer alan "*yukarıdaki fıkrada tanımlanan fiillerin*" ifadesi dikkate alınarak bedeli karşılığı yararlanılan sistemlere girmek suçun ilk fıkrasının yani suçun temel şeklinin kapsamı içine giren şekilde ele alınmıştır. Böylece bedeli karşılığı yararlanılabilen bilişim sistemlerine girilmesi sonucu taksirle verilerin yok olmasına veya değişmesine yol açılırsa doğrudan 243'üncü maddenin 3'üncü fıkrası uygulama alanı bulmalıdır[1].

İkinci yaklaşıma göre ise, TCK'nın 61'inci maddesinin 4'üncü fıkrasını izleyerek bir sonuca ulaşmaktadır. Bu fıkraya göre "*bir suçun temel şekline nazaran daha ağır veya daha az cezayı gerektiren birden fazla nitelikli hallerin gerçekleşmesi durumunda; temel cezada önce artırma sonra indirme yapılır*". Yani hâkim önce 243'üncü maddenin 3'üncü fıkrası uyarınca verilerin yok olması veya değişmesi dikkate alınarak cezada bir artırım yapmalı, daha sonra girilen sistemin bedeli karşılığı yararlanılan sistem olmasından dolayı 2'nci fıkra gereği

[1] Ali Karagülmez, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, 3. Baskı, Ankara, Seçkin Yayıncılık, 2011, s.214

indirime gitmelidir. Doktrinde bir yazar, ilk yaklaşımı kabul ederek böyle bir durumda doğrudan 243/3 uyarınca temel cezada bir artırım yapılması gerektiğini, 3'üncü fıkranın bir neticesi sebebiyle ağırlaşmış hal olduğunu bu sebeple cezayı artıran nitelikli halin olmadığını savunmaktadır[2]. İlk yaklaşımı kabul eden başka bir yazar ise neticesi sebebiyle ağırlaşmış suçu düzenleyen 3'üncü fıkrada suça ilişkin yaptırımın alt ve üst sınırının bulunması sebebiyle 61'inci maddenin 4'üncü fıkrasını uygulama imkânı olmadığını gerekçe olarak belirtmiştir. Yazara göre, failin bu fiilinin birden fazla hükmü ihlal ettiği kabul edilmeli, bu sebeple en ağır cezayı içeren 243/3'ten hüküm kurulmalıdır[3].

Ancak burada nasıl bir yön izleneceği hususunda 243'üncü maddesine bakmak yerinde olacaktır. Maddenin 3'üncü fıkrası 2'inci fıkra bakımından bir istisna getirmemiştir. Öte yandan bakıldığında taksirle verilerin yok olması veya değişmesine yol açılması suçun konusu bakımından önem arz etmemektedir. Bu bağlamda bedeli karşılığı yararlanılan sistemleri de kapsayan bir ifade içeren bu neticesi sebebiyle ağırlaşmış halin gündeme geldiği hallerde 243/3'ün doğrudan uygulanması gerekir[4].

Suçların içtimaına ilişkin genel düzenlemeler ise TCK'nın 42, 43 ve 44'üncü maddelerinde yer almaktadır.

B. Zincirleme Suç

TCK'nın 43'üncü maddesinin 1'inci fıkrası uyarınca aynı suç işleme kararıyla bir kişiye karşı aynı suçun temel halinin veya nitelikli hallerinin değişik zamanlarda işlenmesi halinde zincirleme suç oluşur ve failin cezası artırılır. Bilişim sistemine girme suçu bakımından zincirleme suç hükümlerinin uygulanması mümkündür[5]. Failin bir kişiye ait bilişim sistemine değişik zamanlarda ve aynı suç işleme kararıyla birden fazla kez girmesi veya orada kalması halinde failin cezası dörtte birinden dörtte üçüne kadar artırılacaktır.

Failin çok kısa zaman aralıklarıyla birden fazla kez bilişim sistemine girmesinin zincirleme suç hükümleri kapsamında yer alıp almayacağı hususu tartışılabilir. Örneğin bir

---

[2] **A.e.**, 215.

[3] Yavuz Erdoğan, **Türk Ceza Hukuku'nda Bilişim Suçları**, İstanbul, Legal Yayıncılık, 2013, s. 171-172.

[4] Mahmut Koca, İlhan Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, 5. Baskı, Ankara, Adalet Yayınevi, 2018, s.817.

[5] "Oluşa ve dosya kapsamına göre, bir dönem arkadaşlık yaptığı katılanın şifresini bildiği facebook hesabına rızası dışında girerek, katılanların mesaj içeriklerini alıp aynı suç işleme kararının icrası kapsamında tanıklara gösterdiği ve katılan ...'nın çalıştığı kuruma gönderdiği olayda sanık hakkında TCK'nın 43/1 maddesin uygulanması gerektiğinin gözetilmemesi aleyhe temyiz olmadığından bozma nedeni yapılmamıştır." 12. CD., E. 2015/15370 K. 2017/3455 T. 26.4.2017, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:4.4.2019.

bilişim korsanın mağdurun bilişim sistemine girdikten sonra her seferinde teknik bir nedenle sistemden atılmasına rağmen arka arkaya bilişim sistemine girmesi durumunda kısa zaman aralığında yapılan birden fazla hareketin var olduğu kabul edilebilir. Bu sebeple zincirleme suçtan dolayı tek suçtan dolayı ceza verilip cezasının artırılması gerekir[6]. Nitekim fail kısa aralıklarla da olsa aynı suçu işlemek kastıyla değişik zamanlarda bilişim sistemine girme suçunu işlemiştir.

Öte yandan failin mağdura ait bir donanım aracılığıyla söz konusu donanımın parçasını oluşturduğu bir bilişim sistemine girmesinin ardından bu bilişim sistemi ile bağlanabilmekle birlikte mağdura ait başka program ve yazılımlara erişmesi halinin içtima açısından tartışılması gerekir. Örneğin mağdura ait bir bilgisayara giren failin bilgisayarı açmasının ardından söz konusu donanımla erişilebilmesine rağmen başka sunucularda kayıtlı bulunan e-posta, sosyal medya hesapları ve/veya bulut bilişim sistemlerine erişmesi durumunda failin tek bir bilişim sistemine girme suçundan mı yoksa birden fazla suçtan mı cezalandırılacağı ele alınmalıdır. Her ne kadar suçun konusunun farklı olabileceği kabul edilebilir olsa da[7] hukuki anlamda suçu oluşturan tek bir fiil vardır. Benzer bir durum TCK'nın 141'inci maddesinde düzenlenen hırsızlık suçu bakımından da geçerlidir. Örneğin; aynı mağdura ait olan birden fazla eşyanın fail tarafından mağdurun rızası olmaksızın yarar sağlamak amacıyla alınması halinde tek bir hareket olduğu kabul edilmektedir[8]. Dolayısıyla somut olayın da koşulları dikkate alınarak, mağdura ait bir donanım aracılığıyla bilişim sistemine girildikten sonra ve hala bilişim sisteminde kalmaya devam ederken mağdura ait olan fakat farklı sunucularda kayıtlı olan program ve yazılımlara erişilmesi halinde fail tek bir bilişim sistemine girme suçundan sorumlu olmalıdır.

Failin farklı bilişim sistemlerine girmesi veya bu sistemlerde kalması halinde birden fazla suç oluşacaktır[9]. Fakat aynı mağdura ait farklı bilişim sistemlerine aynı suç işleme kastıyla

---

Murat Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku**, Tamamen Güncellenmiş 7. Baskı, Ankara, Seçkin Yayıncılık, 2018, s. 295. Aynı yönde Doğan Soyaslan, **Ceza Hukuku Özel Hükümler**, 11. Baskı, Ankara, Adalet Yayınevi, 2016, s.638. Aksi yönde; Fatih Selami Mahmutoğlu, "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", **İÜHFM**, C. LXXI, S. 1, s.864.

[7] Avrupa Konseyi Siber Suçlar Sözleşmesinin 1'inci Bölüm 1'inci maddesinin a bendinde "bilgisayar sistemi" ifadesine yer verilmiş ve "bir veya birden fazlası, bir program uyarınca otomatik veri işleyebilen herhangi bir cihaz veya birbiriyle bağlantılı veya ilgili bir grup cihazı ifade eder" şeklinde tanımlanmıştır. Dolayısıyla Avrupa Konseyi Siber Suçlar Sözleşmesi kapsamında birbiriyle bağlantılı veya ilgili grup cihazların hukuken tek bir bilgisayar sistemi olarak kabul edilmesi mümkündür.

[8] Bkz. Kayıhan İçel, **Suçların İçtiması**, İstanbul, İstanbul Üniversitesi Hukuk Fakültesi Yayını, 1972, s.29; Neslihan Göktürk, **Fikri İçtima (Suçların İçtiması)**, Ankara, Adalet Yayınevi, 2013, s.29 vd.

[9] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1417.

farklı zamanlarda girilmesi halinde zincirleme suç oluşmalıdır. Nitekim bilişim sistemi burada suçun konusudur. Aynı mağdura ait olduktan sonra bilişim sistemlerinin farklı olması bu manada farklılık arz etmemelidir. Örneğin; failin mağdura ait fotoğraflara erişmek amacıyla mağdurun önce bilgisayarındaki fotoğraflarına erişip, daha sonraki bir zamanda akıllı telefonundaki fotoğraflara erişmesi halinde zincirleme suç hükümleri uygulanmalıdır.

Failin daha uzun zaman aralığında mağdurun bilişim sistemine girmesi veya orada kalması halinde ise failin aynı suç işleme kararıyla hareket edip etmediğinin tespiti önem arz etmektedir. Doktrinde bir görüşe göre, aynı suç işleme kararından bahsedilemeyecek kadar uzun bir sürenin söz konusu olduğu hallerde failin aynı suç işleme kararıyla hareket etmediği kabul edilmelidir ve gerçek içtima gereğince faile her suç için ayrı ayrı ceza verilmelidir[10]. Ancak bilişim sistemine girme veya orada kalma fiilinin hangi teknik kullanılarak işlendiği somut olay bazında failin aynı suç işleme kastıyla hareket edip etmediğine ışık tutabilir. Örneğin failin mağdura ait bilişim sistemine tekrar tekrar kolaylıkla girmesini sağlayan ve bilişim sistemini bilişim korsanının girişine her an açık tutan "*backdoorların*" tespit edilmiş ve mağdura ait bilişim sistemine birden fazla kez girilmiş olması halinde ilk girişten itibaren uzun bir süre geçmiş olsa da aynı suç işleme kararı olup olmadığının araştırılması gerekir.

Bilişim sistemine girme suçunun diğer bir seçimlik hareketi olan bilişim sisteminde kalma ise mütemadi suçtur ve suç failin bilişim sisteminden çıkmasıyla biter. Dolayısıyla bilişim sisteminde kalma süresi kesilmedikçe failin fiili tek bir suç oluşacaktır[11]. Hâkim ise bilişim sisteminde kalma süresine göre cezaların alt ve üst sınırını dikkate alarak TCK'nın 61'inci maddesi uyarınca cezanın ağırlığını belirleyecektir[12].

C. Fikri İçtima

Bilişim sistemine girme suçu açısından aynı neviden fikri içtimaın uygulanabilmesi de mümkündür[13]. Örneğin fail tek bir e-posta gönderimi ile birden fazla kişiye ait bilişim sistemine trojan gönderebilir. Bu sayede e-posta gönderilen kişilerin bilişim sistemine girebilir veya orada

[10] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 295. Aynı yönde; Yavuz Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, C.12, Özel S., 2012, s.1417, dn.200.
[11] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1417.
[12] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 295; Durmuş Tezcan, Mustafa Ruhan Erdem, R. Murat Önok, **Teorik ve Pratik Ceza Özel Hukuku**, 14. Baskı, Ankara, Seçkin Yayıncılık, 2017, s.984.
[13] Caner Yenidünya, Olgun Değirmenci: **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, İstanbul, Legal Yayıncılık, 2003, s.22.

kalabilir. Bu durumda TCK'nın 43'üncü maddesinin 2'nci fıkrası gereğince failin cezasında artırım yapılacaktır.

Doktrindeki tartışmaların esas noktası bilişim sistemine girme suçu ile diğer bilişim suçlarının fikri içtiması üzerinedir. Bilişim sistemine girme veya orada kalma fiili hemen hemen bütün bilişim suçlarının işlenebilmesi için gerekli bir hareket oluşturmaktadır[14].

Bu konuda doktrinde çeşitli görüşler bulunmaktadır. İlk görüşe göre, bilişim sistemine girme suçu diğer bilişim suçlarının işlenmesi adına zorunluluk oluşturduğu için geçit suçu özelliği taşır. Bu sebeple TCK'da yer alan "*sistemi engelleme, bozma, verileri yok etme veya değiştirme*" suçu (md.244), "*banka veya kredi kartlarının kötüye kullanılması*" suçu (md.245), "*haberleşmenin gizliliğini ihlal*" suçu (md.132)[15], "*kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması*" suçu (md.133), "*özel hayatın gizliliğini ihlal*" suçu (md. 134)[16], "*Kişisel verilerin kaydedilmesi*" suçu (md.135), "*verileri hukuka aykırı olarak verme veya ele geçirme*" suçu (md.136), "*bilişim sistemlerinin kullanılması suretiyle hırsızlık*" suçu (md.142/2-e), "*bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık*" suçu (md.158/1-f) ile 5846 sayılı Fikir ve Sanat Eserleri Kanunu ve 5070 sayılı Elektronik İmza Kanunu'nda düzenlenen bazı suçlarda failin mağdura ait bilişim sistemine hukuka aykırı olarak girerek veya orada kalarak bu suçları işlemesi mümkün olduğu için fail bilişim sistemine girme suçundan değil, ikinci suçtan cezalandırılmalıdır[17].

---

[14] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 295.

[15] Aksi yönde; "Sanıkların sübut bulan bilişim sistemindeki mağdura özel kısma girip, hakları olmadığı halde sistemde kalmaya devam etme eylemlerinin TCK'nın 243/1. maddesinde tanımlanan bilişim sistemine girme ve mağdura ait içeriği özel elektronik iletileri okuyup, tarafı olmadıkları haberleşme içeriklerini kaydetmeleri eylemlerinin TCK'nın 132/1. maddesindeki haberleşmenin gizliliğini ihlal suçlarını oluşturacağı gözetilmeden, suç vasfında yanılgıya düşülerek, sanık ...hakkında TCK'nın 136/1. maddesindeki verileri hukuka aykırı olarak verme veya ele geçirme ve sanık ... hakkında TCK'nın 134/1. maddesindeki özel hayatın gizliliğini ihlal suçundan mahkumiyet kararı verilmesi" hukuka aykırıdır. 12. CD., E. 2014/15082 K. 2015/1624 T. 2.2.2015, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:3.1.2019.

[16]Aksi yönde Yargıtay 12. Ceza Dairesi "Başkasına ait facebook hesabına girerek, arkadaş hanesine bir başka kişiyi ekleme eyleminin sübutu halinde, haberleşmenin gizliliğini ihlal suçunu değil, TCK'nın 243.maddesinde düzenlenen bilişim sistemine girme suçunu oluşturacağı" yönünde karar vermiştir. Karar için bkz. 12. CD., E. 2014/12315 K. 2015/1153 T. 26.1.2015, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:3.1.2019.

Ancak mezkûr karar dikkate alındığında somut olayda her ne kadar haberleşmenin gizliliği ihlal edilmemiş olsa da bilişim sistemine girme suçunun yanı sıra sosyal medya hesabına arkadaş yüklemek suretiyle bilişim sistemine veri yüklenmesi söz konusu olduğundan sanığın 5237 sayılı TCK'nın 244/2 fıkrası gereğince de sorumlu tutulması, icra hareketlerinin örtüşmesi halinde iki suç arasında fikri içtima kurallarının uygulanması gerekmektedir.

[17] Ali Parlar, **Bilişim Alanında İşlenen Suçlar**, Ankara, Bilgi Yayınevi, 2011, s. 21; Soyaslan, **a.g.e.**, s.639; Caner Yenidünya, "Bilişim Sistemine Hukuka Aykırı Erişim Suçu (TCK m.243)", **Legal Fikri ve Sınai Haklar Dergisi**, S.4, 2005, s.1039; Mehmet Emin Artuk, Ahmet Gökcen, Ahmet Caner Yenidünya, **Ceza Hukuku Özel Hükümler**, 15. Baskı, Ankara, Adalet Yayınevi, 2015, s.878; Osman Yaşar, Hasan Tahsin Gökcan, Mustafa Artuç, **Yorumlu-Uygulamalı Türk Ceza Kanunu**, C.5, 2. Baskı, Ankara, Adalet Yayınevi, 2014, s.7295; Şaban Cankat Taşkın,

Diğer bir görüşe göre ise bilişim sistemine girme suçu bazı suçlar bakımından tüketen-tüketilen norm özelliği taşırken, bazı suçlarda bu özelliği göstermemektedir. TCK'da yer alan *"sistemi engelleme, bozma, verileri yok etme veya değiştirme*" suçunun (md.244) işlenebilmesi için failin mağdurun bilişim sistemine girmesi veya orada kalması zorunludur. Dolayısıyla 244'üncü maddede yer alan fiil 243'üncü madde yer alan haksızlık içeriğini de taşıdığından fail yalnızca 244'üncü maddeden sorumlu olmalıdır. Ancak "*bilişim sistemlerinin kullanılması suretiyle hırsızlık*" suçu (md.142/2-e), "*bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık*" suçu (md.158/1-f) gibi suçlarda failin ayrıca 243'üncü maddeden de cezalandırılması gerekmektedir[18].

Ancak bu görüşe göre, "*verileri hukuka aykırı olarak verme veya ele geçirme*" suçu (md.136) diğer bilişim aracılığıyla işlenen suçlardan farklı olarak 243'üncü maddenin haksızlık içeriğini kapsamaktadır ve tüketen-tüketilen norm ilişkisi gereği fail yalnızca 136'ıncı maddeden sorumlu olmadır[19].

Doktrindeki başka bir görüş ise, geçit suç kavramını kabul etmemektedir. Failin hangi suçu işlemeye yönelik kastını dikkate alarak cezai sorumluluğunun belirlenmesi gerektiği ileri sürülmüştür. Buna göre failin amacı bilişim sistemini engellemek, bozmak veya verilerin yok edilmesi ya da değiştirilmesine yönelikse cezai sorumluluğu 244'üncü madde kapsamında değerlendirilmelidir. Fail bilişim sistemine girerek hırsızlık veya dolandırıcılık yapmak kastıyla hareket etmekteyse nitelikli hırsızlık veya nitelikli dolandırıcılıktan sorumlu olmalıdır[20].

Bazı yazarlar ise, böyle bir durumda tek hareketle birden fazla suçun ihlal edildiğini dolayısıyla fikri içtima kurallarının uygulanması gerektiğini savunmaktadır[21]. Farklı neviden fikri içtima açısından bir suçun icra hareketlerinin başka bir suçun icra hareketleriyle kısmen

---

"Karşılaştırmalı Hukukta ve Hukukumuzda Bilişim Suçları", **Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi**, İstanbul, 2008, s.39; Murat Volkan Dülger, **Bilişim Suçları**, Ankara, Seçkin Yayıncılık, 2004, s.225-226. Dülger kitabının ilk basısında yer verdiği bu görüşü daha sonraki basılarda değiştirmiştir.

Korkmaz, haberleşmenin gizliliğini ihlal suçu, kişiler arasındaki konuşmaların dinlenilmesi ve kayda alınması suçu ve özel hayatın gizliliğini ihlal suçu bakımından bilişim sistemine girme suçu ile görünüşte içtimaa tabi olabileceğini savunmaktadır. Ancak örneğin failin bilişim sistemine girdikten belli bir süre sonra verileri kaydetmeye karar verip kaydetmesi halinde gerçek içtimaın uygulanması gerektiğini belirtmektedir. İbrahim Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Ankara, Seçkin Yayıncılık, 2017, s267-268.

[18] Yavuz Erdoğan, "Türk Ceza Kanununda Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", **Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doktora Tezi**, İstanbul, 2011, s.171.

[19] Tezcan/Erdem/Önok, **a.g.e.**, s. 985.

[20] Sacit Yılmaz, **Türk Ceza Hukuku Sisteminde Siber Suçlar**, Ankara, Adalet Yayınevi, 2016, s.190; Veli Özer Özbek v.d., **Türk Ceza Hukuku Özel Hükümler**, 11. Baskı, Ankara, Seçkin Yayıncılık, 2017, s.956.

[21] Akbulut, **Bilişim Alanında Suçlar**, s.152; Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1419.

veya tamamen uyuşması yeterlidir. Bilişim sistemine girme suçunun icra hareketleri olan bilişim sistemine girme veya bilişim sisteminde kalma fiillerini 244'üncü maddede yer sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunun icra hareketleriyle uyuştuğu için daha ağır ceza öngören 244'üncü madde yer alan cezanın uygulanması gerektiği ileri sürülmüştür[22]. Ancak iki suçun icra hareketleri kısmen veya tamamen uyuşmuyorsa farklı neviden fikri içtima söz konusu olmayacak, fail her iki suçtan da ayrı ayrı cezalandırılacaktır[23]. Karakehya da fikri içtimaın mümkün olduğunu kabul etmekle birlikte, failin başkaca suçları işlemek için bilişim sistemine girme suçunu işlemesi halinde TCK'nın 42'nci maddesini temel alarak her iki suçtan da sorumluluğun doğması gerektiğini ileri sürmüştür. Bileşik suçun tanımını yapan 42'nci madde uyarınca "*biri diğerinin unsurunu veya ağırlaştırıcı nedenini oluşturması dolayısıyla tek fiil sayılan*" suçlarda içtima hükmü uygulanmamaktadır. Bunun tersinden anlaşılması gereken ise biri diğerinin unsurunu veya ağırlaştırıcı nedenini oluşturmayan suçlar bileşik suç oluşturmayacağından fail her iki suçtan da sorumlu olmalıdır. Örneğin, "*bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık*" suçunun işlenmesi halinde fail hem bilişim sistemine girme suçundan hem de amaç suç olan nitelikli dolandırıcılıktan sorumlu olmalıdır[24].

Yargıtay bir kararında somut olay bazında geçit suç kavramını kabul etmeyerek failin işlediği suçlardan ayrı ayrı cezalandırılması gerektiğini belirtmiştir. Kararda "*Müştekiye ait banka hesabına, internet üzerinden ulaşılarak, EFT yoluyla başka hesaplara para aktarmak suretiyle gerçekleştirilen eylemin bir bütün halinde TCK'nın 142/2-e maddesinde ifade edilen hırsızlık suçunu oluşturduğu gözetilmeden sanıklar hakkında ayrıca TCK'nın 243/3. maddesindeki suçu oluşturduğundan bahisle yazılı şekilde uygulama yapılması*" kanuna aykırı bulunarak bozma sebebi yapılmıştır[25].

Dülger[26] ise somut olayın koşullarına göre bir değerlendirilme yapılması gerektiğini savunmaktadır. Failin kastının en ağır neticeye yönelik olmadığı ve ilk suçla ağır suçun hukuki değeri korumadığı suçlar bakımından geçit suçu söz konusu olmayacaktır[27]. Dolayısıyla bilişim

---

[22] Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, s.819. Sevük, haberleşmenin gizliliğini ihlal suçunun bilişim sistemine girme suçu ile birlikte işlenmesi halinde fikri içtimaın uygulanması gerektiğini savunmaktadır. Handan Yokuş Sevük, **Türk Ceza Hukuku Özel Hükümler**, Ankara, Adalet Yayınevi, 2018, s. 237,

[23] **A.e.**, s.818

[24] Hakan Karakehya, "Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu", **TBB Dergisi**, Sayı 81, 2009, s.21.

[25] Aynı yönde nitelikli hırsızlık ve bilişim sistemine girme suçunun ayrı ayrı cezalandırılmasıyla ilgili bkz. 13. CD., E. 2014/2924 K. 2014/36282 T. 18.12.2014, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:4.4.2019. Aynı yönde bkz. 13. CD., E. 2014/23539 K. 2015/8515 T. 6.5.2015; 17. CD., E. 2016/10724 K. 2018/12290 T. 10.10.2018.

[26] Dülger kitabının ilk basısında yer verdiği bu görüşü daha sonraki basılarda değiştirmiştir.

[27] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 299.

sistemine girme suçuyla korunan hukuki değerle aynı hukuki değeri koruyan 244'üncü madde hariç diğer suç tipleri açısından geçit suç kavramı kabul edilemez[28]. 244'üncü madde bağlamında da suçun nasıl işlendiği önem arz etmektedir. Örneğin, bir sabit diski suyla temas ettirerek işlevsiz hale getirilmesi ile verilerin yok edilmesi halinde 244'üncü maddenin gerçekleşmesi için bilişim sistemine girme suçu geçit suç ilişkisini taşımayacaktır[29]. Yazar, fikri içtima açısından da benzer bir düşünceyle somut olaya bakılması gerektiğini savunmaktadır. Fikri içtima kapsamında failin tek hareketinden bahsedilebilmesi için fiiller arasında zamansal bir yakınlığın mevcut olması gerekir. Dolayısıyla somut olayda failin bilişim sistemine girme suçunu işlemesiyle diğer suçları işlemesi arasında zamansal bir farklılık olması halinde farklı neviden fikri içtima hükmünün uygulanması söz konusu olmayacaktır[30].

Görünüşte içtimaın bir türü olan asli norm-tali norm ilişkisi bağlamında bir suçun diğer suç açısından yardımcı norm olup olmadığı kanunda açıkça belirtilmemiş olabilir[31]. Geçit suçun söz konusu olabilmesi için doktrinde bazı şartlara yer verilmiştir. Bu sebeple geçit suça ilişkin şartlar belirtilirken yukarıda anılan suçlar açısından bilişim sistemine girme suçunun geçit suç olup olamayacağı ortaya konulmalıdır.

Öncelikle geçit suç için bir suçu işlemek amacıyla başka bir suçun geçilmesi gerekir. Bu hallerde önceki hareketin cezalandırılmaması için işlenen her iki suçun da aynı hukuki değeri koruması gerekmektedir[32]. Bu bakımdan 244/1-2'nci fıkralar hariç diğer suçlarda farklı hukuki değerler gündeme gelmektedir[33]. Geçit suç kavramının tartışılabileceği diğer suçların da korunan hukuki değerini ortaya koymak gerekir. Banka veya kredi kartlarının kötüye kullanılması suçu (md.245) ile korunan hukuki değer hem malvarlığına ilişkin hakları hem de ticari hayatı kapsayan kamu düzeni ve güveliğini içeren haklar olarak ifade edilebilir ve karma niteliklidir. Haberleşmenin gizliliğini ihlali suçu (md.132) ile korunan hukuki değer ise haberleşme hürriyetidir[34]. Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçu (md.133) ve özel hayatın gizliliğini ihlal suçu (md. 134) ile korunan hukuki değerler ise temel

---

[28] **A.e.**

[29] **A.e.**, s.300.

[30] **A.e.**, s.300.

[31] Kayıhan İçel, "Görünüşte Birleşme (İçtima) İlkeleri ve Yeni Türk Ceza Kanunu", **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi**, Y. 7, S. 14, Güz 2008, s. 42.

[32] **A.e.**, s.46.

[33] Bkz. Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 299.

[34] Korkmaz, **a.g.e.**, s.317. Başka bir görüşe göre ise burada korunan hukuki değer haberleşmenin gizliliği ve mahremiyetidir. Bkz. Mahmut Koca, "Haberleşmenin, Konuşmanın ve Özel Hayatın Gizliliğini İhlal Suçları (TCK m.132-134)", **Ceza Hukukunun Güncel Sorunları**, Erzurum, 8 Ekim 2010, s.66-67.

olarak kişilerin özel hayatının gizliliğidir[35]. Kişisel verilerin kaydedilmesi suçu (md.135) ve verileri hukuka aykırı olarak verme veya ele geçirme suçunda (md.136) korunan hukuki değerler genel olarak özel hayatın gizliliği, özel olarak ise kişisel verilerin korunmasıdır[36]. Bilişim sistemlerinin kullanılması suretiyle hırsızlık suçu (md.142/2-e) ve bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçu (md.158/1-f) açısından korunan hukuki değerler ise genel olarak malvarlığına ilişkin değerler olarak kabul edilebilir[37]. Karşılıksız yararlanma suçu (md. 163) ile korunan hukuki değer de yine malvarlığına yönelik haklardır[38].

5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun 1-B maddesinin g bendi uyarınca bilgisayar programları da bu Kanun kapsamında sayılmış, aynı Kanunun "*manevi, mali veya bağlantılı haklara tecavüz*" başlıklı 71'inci maddesi "*bu Kanunda koruma altına alınan fikir ve sanat eserleriyle ilgili manevi, mali veya bağlantılı hakları ihlal ederek*" "*hak sahibi kişilerin yazılı izni olmaksızın işleyen, temsil eden, çoğaltan, değiştiren, dağıtan, her türlü işaret, ses veya görüntü nakline yarayan araçlarla umuma ileten, yayımlayan ya da hukuka aykırı olarak işlenen veya çoğaltılan eserleri satışa arz eden, satan, kiralamak veya ödünç vermek suretiyle ya da sair şekilde yayan, ticarî amaçla satın alan, ithal veya ihraç eden, kişisel kullanım amacı dışında elinde bulunduran ya da depolayan*" kişinin cezalandırılacağı hükme bağlanmıştır. Söz konusu suç bilişim sistemine girme suçu ile birlikte işlense dahi Kanun metninden de anlaşılacağı üzere burada korunan hukuki değerler genel olarak "*fikir ve sanat eserleriyle ilgili manevi, mali veya bağlantılı*"[39] haklar[40], bilgisayar programları için mali haklardır[41]. 5070 sayılı Elektronik İmza Kanunu'nun 16'ıncı maddesi uyarınca ise "*Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar*" cezalandırılmaktadır.

---

[35]Korkmaz, **a.g.e.**, s. 318, 320. Koca'ya göre ise burada korunan hukuki değer sözün mahremiyetidir. Bkz. Koca, **a.g.m.**,s.84.

[36] Dülger, Murat Volkan: "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması", İ**stanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, S.3 (2), Güz 2016, s. 101-167.

[37] Özbek v.d., **a.g.e.**, s.610,710.

[38] Bkz. Özen Kaya, "5237 Sayılı Türk Ceza Kanunu'nda Karşılıksız Yararlanma Suçu", **Gazi Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi,** Ankara, (Çevrimiçi), tez.yok.gov.tr, 2011, Erişim Tarihi:12.4.2019, s.22.

[39] Aynı yönde; Hüseyin Çakır, Mehmet Serkan Kılıç, **Güncel Tehdit: Siber Suçlar**, Ankara, Seçkin Yayıncılık, 2014, s.192.

[40] Bkz. Esra Dikmen, "Manevi, Mali veya Bağlantılı Haklara Tecavüz Suçları (FSEK m. 71/1-1)", **İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi**, İstanbul, 2018, s.68 vd.

[41] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s.504.

Burada korunan hukuki değerin ise kamunun elektronik imza ile onaylanan belgelere ve bunların doğruluğuna duyulan güven olduğu ifade edilebilir[42].

Bilişim sistemine girme suçu ile korunan hukuki değer ise bilişim sisteminin güvenliği ve güvenilirliğidir. Dolayısıyla bilişim sistemine girme suçu yukarıda anılan suç tiplerinin hiçbiri ile aynı hukuki değeri korumadığı için geçit suç olarak değerlendirilemeyecektir. Bilişim sistemine girme suçu ile yukarıda anılan suçlara ilişkin hareketlerin tamamının veya bir kısmının aynı hareketle gerçekleştirilmesi halinde farklı neviden fikri içtima söz konusu olabileceği gibi, bu hareketlerin kesişmemesi yani tek hareket olarak değerlendirilememesi halinde ise gerçek içtima uygulanarak failin her iki suçtan da ayrı ayrı cezalandırılması gündeme gelebilecektir[43]. TCK'nın 244/1-2'nci fıkralarında yer alan suçlar bakımından korunan farklı hukuki değerler gündeme gelebilse de bilişim sisteminin güvenliğinin de bu fıkralar kapsamında korunduğu kabul edilebilir nitelikte olduğundan geçit suçun diğer şartları açısından değerlendirme yapmak gerekir.

Bir suçun işlemesi için başka bir suçun içinden geçilmesi gereken hallerde failin kastının mutlaka ağırlaşan sonucun gerçekleşmesine yönelik olması gerekmektedir[44]. Bu bakımdan 244/1-2'nci fıkralarda yer alana suçların işlenmesi amacıyla 243'üncü maddenin işlenmesi hali geçit suç bakımından bu şartı sağlamaktadır. Ancak sadece bu koşulun sağlanması geçit suçun varlığını kabul etmeye yetmeyecektir.

Belirtmek gerekir ki ağır sonuca yönelik suçun işlenmesi için içinden geçilen suç, işlenmek istenen suçun hazırlık hareketi olmamalıdır. Burada ayrıca TCK'nın 245/A

---

[42] **A.e.**, s.527.

[43] Yargıtay bazı kararlarında bilişim sistemine girme suçu ile bilişim aracılığıyla işlenen suçların ayrı ayrı ele alınması gerektiğini belirtmiştir. "Sanık hakkında 08/02/2010 tarih ve 2009/5363 soruşturma numaralı iddianame ile hukuka aykırı olarak bilişim sistemine girme ve orada kalma suçundan TCK'nın 243/1 maddesi uyarınca kamu davası açılmasına rağmen bu suçla ilgili tartışma ve değerlendirme yapılmadığı gibi hüküm de kurulmadığı anlaşıldığından, zamanaşımı içerisinde işlem yapılması mümkün görülmüştür.
Sanık ...'ın, hakkında mahkumiyet kararı verilen ve temyiz kapsamında olmayan diğer sanık... ile birlikte, ..., ... ve ...'a ait MSN Messenger adreslerinin şifresini ele geçirip farklı zamanlarda internete girerek MSN adreslerindeki arkadaş listesinde bulunan kişilerden acil olarak kontör istedikleri, ...'in arkadaşı olan şikayetçi ...'in 12 adet, ...'un dayısının kızı olan şikayetçi ...'in 1 adet, ...'in de öğrencisi olan şikayetçi...'in 2 adet 250'lik kontör şifresini bilgisayara yazıp gönderdikleri, gönderilen kontör şifrelerinin sanıklar tarafından piyasada ucuza satıldığı şeklinde gerçekleşen eylemlerinin nitelikli dolandırıcılık suçlarını oluşturduğu anlaşıldığından mahkemenin kabulünde bir isabetsizlik görülmemiştir." 15. CD., E. 2016/4937 K. 2017/19032 T. 28.9.2017, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:3.4.2019.

[44] Zafer İçer, "Türk Ceza Hukukunda Tüzel Kişiler", **Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi**, İstanbul, 2011, s.47.

maddesinde yer alan "*yasak cihazlar ve programlar*" suçunun değerlendirilmesi gerekir[45]. Söz konusu maddeye göre "*bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır*".

Bilişim sistemine girme suçunu işlemek amacıyla söz konusu maddede anılan yasak cihaz ve programları imal edip veya bulundurup kullanan kişi bakımından bu suç bir araç suç özelliği taşıyacaktır[46]. Öte yandan bu yasak cihaz ve programlar bilişim sistemine girme suçu için bir hazırlık hareketi olarak değerlendirilebileceğinden gerçek içtima kurallarına tabi tutulacaktır.

Her ne kadar farklı hukuki değerler korunduğu için geçit suç söz konusu olamayacak olsa da belirtmek gerekir ki 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun 72'nci maddesinde düzenlenen "*koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri*" başlıklı suç ile "*bir bilgisayar programının hukuka aykırı olarak çoğaltılmasının önüne geçmek amacıyla oluşturulmuş, ilave programları etkisiz kılmaya yönelik program veya teknik donanımları üreten, satışa arz eden, satan veya kişisel kullanım amacı dışında elinde*" bulundurmak da hazırlık hareketleri olarak değerlendirilebileceğinden bu suç ile bilişim sistemine girme suçunun işlenmesi halinde fail her iki suçtan da cezalandırılmalıdır.

Geçit suçtan söz edebilmek için ağırlaşan sonucun gerçekleşmesinde geçilen hafif suçun işlenmesinin zorunlu olması gerekir[47]. Bu bağlamda aynı hukuki değerin korunmadığı suçlar açısından ayrıca bir zorunluluk değerlendirilmesi yapılmasına gerek yoktur. Ancak 244/1-2'nci fıkralar açısından bilişim sistemine girme suçunun zorunlu olup olmadığının incelenmesi gerekir. Sistemi engelleme, bozma veya verileri yok etme, değiştirme suçlarının işlenmesi için bilişim sistemine girme suçunun her zaman zorunlu olduğundan bahsedilemeyecektir. Örneğin, bilgisayarın çekiçle kırılması veya hard diskin sıvı içine atılarak bozulması hareketleriyle fail 244/1-2'nci fıkralarda yer alan suçlarda yer alan seçimlik hareketlerden bazılarını bilişim

[45] Bkz. . Zafer İçer, "Suça Teşebbüste Hazırlık Hareketleri ile İcra Hareketlerinin Birbirinden Ayrılması Meselesi", **Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doktora Tezi**, İstanbul, 2017, s. 66.
[46] Akbulut, **Bilişim Alanında Suçlar**, s.153.
[47] İçel, **a.g.m**., s.47.

sistemine girmeksizin işleyebilmektedir[48]. Ancak failin bilgisayara trojan göndererek bilgisayar işletim sisteminin çökmesine yol açması veya sistemde yer alan dosyaları yok etmesi halinde fail 244/1-2'nci fıkralarında yer alan suçları işlemek için zorunlu olarak bilişim sistemine girme suçunu da işlemiştir. Doktrinde somut olay çerçevesinde geçit suç söz konusu olduğu için fail yalnızca 244'üncü maddeden sorumlu olması gerektiği ileri sürülmüştür[49]. Ancak burada somut olay bazında bir zorunluluk aranması gerektiği mi yoksa genel olarak tüm ihtimaller dâhilinde ağır sonuca yönelik suçun işlenmesi için geçit olarak kullanılan hafif suçun işlenmesi zorunluluğunun mu olması gerektiği sorusunun cevaplanması gereklidir.

Dolayısıyla TCK'nın gerek 244'üncü maddesinin 1'inci fıkrasında yer alan bilişim sisteminin işleyişini engelleme ve bozma gerekse 2'nci fıkrada yer alan bilişim sistemindeki verileri değiştirme veya erişilmez kılma, sisteme veri yerleştirme ve var olan verileri başka bir yere gönderme bakımından somut olaya göre değil seçimlik harekete göre bir değerlendirme yapılması gerekir. Bu bağlamda 244'üncü maddenin 1'inci fıkrası bakımından bilişim sisteminin işleyişini engelleme seçimlik hareketinin işlenmesi ile 244'üncü maddenin 2'nci fıkrasında yer alan bilişim sistemindeki verileri değiştirme, sisteme veri yerleştirme veya var olan verileri başka bir yere gönderme seçimlik hareketleri bakımından bilişim sistemine girme suçunun işlenmesinin zorunlu olduğu kabul edilebilir[50].

Yargıtay bilişim sisteminde şifre değişikliğinin söz konusu olduğu olaylarda 243'üncü madde ile 244'üncü maddenin içtimaı konusunda farklı kararlar vermiştir. Yargıtay 12. Ceza Dairesi'nin TCK'nın 244/2'nci fıkrası ile 243'üncü maddesi arasında geçit suç olduğu sonucuna ulaştığı bir kararına göre; "*Sanık ...'un, mağdurlar ... ve ...'ya ait MSN adreslerinin ve facebook hesaplarının internet şifrelerini, onların rızası dışında değiştirerek, mağdurların bilişim sistemindeki hesaplarına erişimlerini engellemesi şeklinde sübutu kabul edilen eylemlerinden dolayı TCK'nın 244/2. madde ve fıkrasında tanımı yapılan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan mağdur sayısınca iki ayrı mahkumiyet hükmü kurulması ve MSN ile facebook hesaplarının iki farklı bilişim sistemi olmasından dolayı*

---

[48] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 300.

[49] **A.e.**, s. 300.

[50] Dülger diğer seçimlik hareketler için somut olaya göre değerlendirme yapılması gerektiğini ileri sürmektedir. bkz. Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 298.
Yazıcıoğlu, 243'üncü madde ile 244'üncü madde arasında zorunluluk unsurunun oluştuğu gerekçesiyle geçit suç söz konusu olduğunu, bu sebeple failin yalnızca ağır suçtan sorumluluğun doğması gerektiğini savunmaktadır. Bkz. Yılmaz Yazıcıoğlu, "Hackerler ve Bilişim Sistemine Girme Suçu", **Ord. Prof. Dr. Sulhi Dönmezer Armağanı**, C.II, Ankara, Atatürk Kültür, Dil ve Tarih Yüksek Kurumu, Atatürk Araştırma Merkezi ve Türk Ceza Hukuku Derneği Yayını, s. 1260.

bir suç işleme kararının icrası kapsamında değişik zamanlarda her bir mağdura karşı aynı eylemi birden fazla işleyen sanık hakkında TCK'nın 43/1. madde ve fıkrasında düzenlenen zincirleme suç hükmünün uygulanması gerektiği gözetilmeden, sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan tek bir mahkumiyet hükmü kurulup, zincirleme suç hükümlerinin uygulanmaması ve olayda uygulama alanı bulunmayan TCK'nın 243/1. madde ve fıkrasındaki bilişim sistemine girme suçundan da ayrıca mahkumiyet hükmü kurulması" hukuka aykırıdır[51].

Yargıtay başka şifre değiştirmenin söz konusu olduğu bir kararında bilişim suçuna girme suçunun yanında ayrıca TCK'nın 244'üncü fıkrasından hüküm kurulması gerektiği yönünde görüş beyan etmiştir. Karara göre, "*sanığın katılan ...'in hesaplarının şifresini ele geçirip, ardından şifreleri değiştirmesi şeklindeki eylemi ile şikayetçi ...'dan para istemesi eyleminin iki ayrı suçu oluşturması karşısında; TCK'nın 44. maddesinin uygulanma imkanının bulunmadığı, ayrıca iddia makamının talep ettiği kanun maddesinin sanık için kazanılmış hak oluşturmayacağı da göz önüne alındığında, tebilğnamedeki TCK'nın 243/1 maddesi gereğince bozma isteyen düşünceye iştirak edilmemiş olup, sanığın katılan ...'in e posta adresinin ve facebook hesabının şifresini kırması, ardından da şifreyi değiştirmesi şeklindeki eyleminden dolayı TCK'nın 244/2 maddesinde düzenlenen bilişim sistemindeki verileri bozma yok etme, erişilmez kılma, sisteme veri yerleştirme suçundan da mahkumiyet kararı verilmesi gerekirken yazılı şekilde hüküm kurulması*" hukuka aykırıdır kararı verilmiştir[52].

TCK'nın 244'üncü maddesinin 1'inci ve 2'nci fıkrasında yer alan seçimlik hareketler aynı zamanda serbest hareketli suçlar olduğu için failin fiilinin her iki fıkrada yer alan seçimlik harekete de girmesi mümkündür. Böyle bir durumda 1'inci fıkra 2'nci fıkraya göre daha

---

[51] 12. CD., E. 2016/10818 K. 2017/7390 T. 11.10.2017, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:3.4.2019.

[52] 15. CD., E. 2017/31912 K. 2018/2652 T. 17.4.2018, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:3.4.2019.
Aynı yönde bkz. "Sanığın katılanın şifresini kırmak suretiyle girdiği facebook hesabında katılan tarafından yazılmış intiba uyandıracak biçimde ve katılanı küçük düşürücü ifadeler yazma şeklindeki eyleminin TCK'nın 244/2. maddesinde düzenlenen bilişim sistemine veri yerleştirme suçunu oluşturduğu gözetilmeden, hukuki nitelendirmede hataya düşülmek suretiyle sanığın TCK'nın 243/1. maddesi gereğince cezalandırılmasına ve ayrıca bilişim sistemine veri yerleştirme suçundan dolayı suç duyurusunda bulunulmasına karar verilmiş ise de, karşı temyiz olmadığından bozma yapılamayacağı" 4. CD., E. 2013/19106 K. 2014/14018 T. 28.4.2014, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:3.4.2019.
"Katılan şirketin sistemine hukuka aykırı olarak girerek, sistemin işleyişini engelleme, bozma, sistemdeki verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme şeklindeki TCK.nun 244/1-3. madde ve fıkralarında yazılı hallerin gerçekleşmemesi nedeniyle, anılan mad- denin 4. fıkrasının uygulanamayacağı, katılan şirkete ait sisteme hukuka aykırı olarak girme ve orada kalmaya devam etme şeklindeki eylemin TCK.nun 243/1. madde ve fıkrasında düzenlenen suçu oluşturacağının gözetilmemesi, Yasaya aykırı", 8. CD., E. 2016/104 K. 2016/7753 T. 13.6.2016, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:3.4.2019.

öncelikli konumda yer aldığı için 1'inci fıkranın uygulanması gerekir[53]. Bir bilişim sistemine ait şifrenin değiştirilmesi Yargıtay uygulamalarında farklılık arz etse de, TCK'nın 244'üncü maddesi bakımından ilk fıkrada yer alan bilişim sisteminin işleyişinin engellenmesi seçimlik hareketini de oluşturacağından şifrenin değiştirilmesi halinde 244/1 gereğince hüküm kurulması gerekmektedir[54]. Bu sebeple bilişim sistemine girilerek şifre değiştirilmesi halinde geçit suç bakımından zorunluluk unsuru oluşmayacağından 243'üncü maddeyle 244/1'inci maddeden cezai sorumluluğun doğması gerekir.

Yargıtay 4. Ceza Dairesi ise "*Sanığın katılanın şifresini kırmak suretiyle girdiği facebook hesabında katılan tarafından yazılmış intiba uyandıracak biçimde ve katılanı küçük düşürücü ifadeler yazma şeklindeki eyleminin TCK'nın 244/2. maddesinde düzenlenen bilişim sistemine veri yerleştirme suçunu oluşturduğu gözetilmeden, hukuki nitelendirmede hataya düşülmek suretiyle sanığın TCK'nın 243/1. maddesi gereğince cezalandırılmasına ve ayrıca bilişim sistemine veri yerleştirme suçundan dolayı suç duyurusunda bulunulmasına karar verilmiş ise de, karşı temyiz olmadığından bozma yapılamayacağı*" yönünde karar vermiştir. Ancak sanığın sosyal medya hesabına veri yükleyebilmesi için mevcut teknolojik gelişmeler altında sosyal medya hesabına girmesi zorunludur. Dolayısıyla 244/2 fıkrası kapsamındaki sisteme veri yerleştirme seçimlik hareketinin işlenmesi için bilişim sistemine girme suçundan geçilmesi gerektiğinden failin yalnızca 244/2'den cezai sorumluluğunun doğması gerekmektedir.

Diğer yandan ağır suçun fail ve mağdurunun hafif suçun fail ve mağduruyla aynı olması zorunludur. Önceki hafif suçla sonraki ağır suçun fail ve mağdurlarının farklı olması halinde her fiil bağımsız olarak değerlendirilecektir[55]. Bilişim sistemine girme suçundan geçilerek bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçunun işlenmesi halinde hâkim somut olayda fail ve mağdurların kim olduğunu tespit ederek geçit suçun olup olmadığına karar vermelidir.

Geçit suçun varlığı için aranan diğer bir koşul ise, ağırlaşan sonuç ile failin bu sonuca yönelik hareketinde tek bir nedensellik bağının olması gerekir[56]. Yine belirtmek gerekir ki geçit suçun söz konusu olduğu hallerde failin kastı baştan itibaren ağırlaşan neticeye yönelik olduğu

---

[53] Karagülmez, **a.g.e**., s.239.
[54] Bkz. Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 298,332.
[55] İçel, **a.g.m**., s.47.
[56] **A.e.**

için ağır sonucun meydana gelmemesi halinde fail ağır suça teşebbüsten sorumlu olmalıdır[57]. Örneğin bilişim sisteminde yer alan verileri değiştirmek amacıyla bilişim sistemine giren fail verilere müdahale edecekken elektriklerin kesilmesi halinde bilişim sistemine girme suçundan değil, bilişim sisteminde yer alan verileri değiştirme veya yok etme suçuna teşebbüsten sorumlu tutulmalıdır.

Sonuç olarak, sistemde bulunan verilerin değiştirilmesi, sisteme veri yerleştirilmesi veya var olan verilerin başka bir yere gönderilmesi seçimlik hareketlerinin işlenmesiyle TCK'nın 244'üncü maddesinin 2'nci fıkrasında yer alan suçun oluşumuna meydan verilmesi halinde bilişim sistemine girme suçunun geçit suç olduğu kabul edilebilir. Ancak teknolojinin gelişimi de dikkate alınmalıdır. Bu noktada bilişim sistemine girmeksizin sistemde bulunan verilerin değiştirilmesi, sisteme veri yerleştirilmesi veya var olan verilerin başka bir yere gönderilmesini mümkün kılan bir teknolojinin varlığında artık zorunluluk unsuru ortadan kalkacağından geçit suçun varlığından da bahsedilemeyecektir.

Yukarıda ayrıntılı şekilde açıklandığı üzere görünüşte içtima için suçların haksızlık muhtevalarının örtüşmesi gerekmektedir[58]. Ancak yukarıda anılan diğer suçlarla bilişim sistemine girme suçunun haksızlık muhtevası örtüşmediği için görünüşte içtima gündeme gelmeyecektir. Ancak birden fazla suçun icra hareketlerinin kısmen veya tamamen örtüşmesi halinde farklı neviden fikri içtimaın kabulü gerekir[59]. İcra hareketlerinin örtüşmemesi halinde ise fail hem bilişim sistemine girme suçundan hem de işlediği diğer suçtan ayrı ayrı cezalandırılmalıdır.

---

[57] **A.e.**, s.48.

[58] Göktürk, **Fikri İçtima (Suçların İçtiması)**, s.76.

[59] Görünüşte içtima ile fikri içtimaın farklarının sonuçları vardır. Bu bakımdan bu ayrımın yapılması önem arz etmektedir.
Görünüşte içtima halinde suçlar gerçek anlamda içtima ettirilmediğinden yalnızca cezalandırılması gereken suçun kararda anılması yeterliyken fikri içtima da içtima ettiren suçların hepsinin anılması gerekir. Diğer bir sonuç ise cezanın belirlenmesi açısındandır. Görünüşte içtimada yalnızca bir suç işlendiği kabul edildiğinden cezanın bireyselleştirilmesinde cezalandırılmayan suç önem arz etmez. Ancak fikri içtimada fikri içtimaya tabi tutulan suçlar cezanın bireyselleştirilmesine etki etmektedir. Son olarak görünüşte içtimada zamanaşımı cezalandırılan suçtan itibaren başlarken fikri içtimada ise her suç bakımından ayrı ayrı işlemektedir. Bkz. Göktürk, **Fikri İçtima (Suçların İçtiması)**, s.75-76.

KAYNAKÇA

Akbulut, Berrin: **Bilişim Alanında Suçlar**, Ankara, Adalet Yayınevi, 2017.

Artuk, Mehmet Emin, Ahmet Gökcen, Ahmet Caner Yenidünya: **Ceza Hukuku Özel Hükümler**, 15. Baskı, Ankara, Adalet Yayınevi, 2015.

Çakır, Hüseyin, Mehmet Serkan Kılıç: **Güncel Tehdit: Siber Suçlar**, Ankara, Seçkin Yayıncılık, 2014.

Dikmen, Esra: "Manevi, Mali veya Bağlantılı Haklara Tecavüz Suçları (FSEK m. 71/1-1)", **İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi**, İstanbul, 2018.

Dülger, Murat Volkan: "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması", **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, S.3 (2), Güz 2016,

Dülger, Murat Volkan: **Bilişim Suçları ve İnternet İletişim Hukuku**, Tamamen Güncellenmiş 7. Baskı, Ankara, Seçkin Yayıncılık, 2018.

Dülger, Murat Volkan: **Bilişim Suçları**, Ankara, Seçkin Yayıncılık, 2004.

Erdoğan, Yavuz: "Bilişim Sistemine Girme ve Kalma Suçu", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, C.12, Özel S., 2012, s.1363-1433.

Erdoğan, Yavuz: "Türk Ceza Kanununda Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", **Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doktora Tezi**, İstanbul, 2011.

Erdoğan, Yavuz: **Türk Ceza Hukuku'nda Bilişim Suçları**, İstanbul, Legal Yayıncılık, 2013.

Göktürk, Neslihan: **Fikri İçtima (Suçların İçtiması)**, Ankara, Adalet Yayınevi, 2013.

İçel, Kayıhan: **Suçların İçtiması**, İstanbul, İstanbul Üniversitesi Hukuk Fakültesi Yayını, 1972.

İçer, Zafer: "Suça Teşebbüste Hazırlık Hareketleri ile İcra Hareketlerinin Birbirinden Ayrılması Meselesi", **Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doktora Tezi**, İstanbul, 2017.

İçer, Zafer: "Türk Ceza Hukukunda Tüzel Kişiler", **Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi**, İstanbul, 2011.

Karagülmez, Ali: **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, 3. Baskı, Ankara, Seçkin Yayıncılık, 2011.

Karakehya, Hakan: "Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu", **TBB Dergisi**, Sayı 81, 2009.

Kaya, Özen: "5237 Sayılı Türk Ceza Kanunu'nda Karşılıksız Yararlanma Suçu", **Gazi Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi,** Ankara, (Çevrimiçi), tez.yok.gov.tr, 2011, Erişim Tarihi:12.4.2019.

Kayıhan İçel, "Görünüşte Birleşme (İçtima) İlkeleri ve Yeni Türk Ceza Kanunu", **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi**, Y. 7, S. 14, Güz 2008.

Koca, Mahmut, İlhan Üzülmez: **Türk Ceza Hukuku Genel Hükümler**, 11. Baskı, Ankara, Adalet Yayınevi, 2018

Koca, Mahmut, İlhan Üzülmez: **Türk Ceza Hukuku Özel Hükümler**, 5. Baskı, Ankara, Adalet Yayınevi, 2018.

Koca, Mahmut: "Haberleşmenin, Konuşmanın ve Özel Hayatın Gizliliğini İhlal Suçları (TCK m.132-134)", **Ceza Hukukunun Güncel Sorunları**, Erzurum, 8 Ekim 2010.

Korkmaz, İbrahim: **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Ankara, Seçkin Yayıncılık, 2017.

Mahmutoğlu, Fatih Selami: "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", **İÜHFM**, C. LXXI, S. 1, s. 891-890.

Özbek, Veli Özer, Koray Doğan, Pınar Bacaksız, İlker Tepe: **Türk Ceza Hukuku Özel Hükümler**, 11. Baskı, Ankara, Seçkin Yayıncılık, 2017.

Parlar, Ali: **Bilişim Alanında İşlenen Suçlar**, Ankara, Bilgi Yayınevi, 2011.

Sevük, Handan Yokuş: **Türk Ceza Hukuku Özel Hükümler**, Ankara, Adalet Yayınevi, 2018.

Soyaslan, Doğan: **Ceza Hukuku Özel Hükümler**, 11. Baskı, Ankara, Adalet Yayınevi, 2016.

Taşkın, Şaban Cankat: "Karşılaştırmalı Hukukta ve Hukukumuzda Bilişim Suçları", **Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi**, İstanbul, 2008.

Tezcan, Durmuş, Mustafa Ruhan Erdem, R. Murat Önok: **Teorik ve Pratik Ceza Özel Hukuku**, 14. Baskı, Ankara, Seçkin Yayıncılık, 2017.

Yaşar, Osman, Hasan Tahsin Gökcan, Mustafa Artuç: **Yorumlu-Uygulamalı Türk Ceza Kanunu**, C.5, 2. Baskı, Ankara, Adalet Yayınevi, 2014.

Yazıcıoğlu, Yılmaz: "Hackerler ve Bilişim Sistemine Girme Suçu", **Ord. Prof. Dr. Sulhi Dönmezer Armağanı**, C.II, Ankara, Atatürk Kültür, Dil ve Tarih Yüksek Kurumu, Atatürk Araştırma Merkezi ve Türk Ceza Hukuku Derneği Yayını, s. 1239-1261.

Yenidünya, Caner, Olgun Değirmenci: **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, İstanbul, Legal Yayıncılık, 2003.

Yenidünya, Caner: "Bilişim Sistemine Hukuka Aykırı Erişim Suçu (TCK m.243)", **Legal Fikri ve Sınai Haklar Dergisi**, S.4, 2005, s.1018-1042.

Yılmaz, Sacit: **Türk Ceza Hukuku Sisteminde Siber Suçlar**, Ankara, Adalet Yayınevi, 2016.

Mahmut Koca, İlhan Üzülmez, **Türk Ceza Hukuku Genel Hükümler**, 5. Baskı, Ankara, Adalet Yayınevi, 2018, s.685.

ÖZEL HAYATIN GİZLİLİĞİ KAPSAMINDA KİŞİSEL VERİLERİN KULLANIMININ SINIRLARI

Doç.Dr. Pınar Memiş Kartal[•]

Özel hayatın bir parçası olarak kabul edilen kişisel verilerin, özel hayattan bağımsız bir hak olarak nitelendirilmesi gerektiği bilincine ulaşıldığı günümüzde, bu verilerin toplanmasının, depolanmasının ve kötü niyetli kişilerce kullanılmasının büyük ölçüde yaratacağı sıkıntılar her geçen gün daha fazla konuşulmakta ve bu keyfiyetin kontrolü için çalışmalar yapılmaktadır. Bu çalışmaların başında elbette hukuki çözüm arayışları gelmektedir. Temel hak ve özgürlüklere keyfi müdahalelerin yasak olduğu konusunda hemfikir olunduğu bir konunun çözümü de elbette hukuki olacaktır. Ancak kişisel verilerin kullanımı o kadar çeşitlidir ki bu alanda hukuki düzenleme yapabilmek ve sonrasında keyfi müdahale ile mücadelede yöntemler geliştirmek, farklı disiplinlerle de sıkı bir çalışmayı gerektirmektedir. Bunun başında elbette internet, bilişim, veri bankaları ve aslında genel ifadesiyle teknoloji gelmektedir.

Temel bir insan hakkı konusu ve ihlali ile sorunu olarak kabul edilen özel hayatın gizliği ve bu bağlamdan kişisel veriler doğrudan insan onuru ile bağlantılıdır. Teknoloji ile kişisel verilerin ilgilinin rızası olmaksızın kullanılması yaygındır ancak tek kullanım aracı elbette değildir. Münferit kullanımlar, teknolojiden yararlanmaksızın kişilerin verilerinin ele geçirilmesi de mümkündür ve hatta bu veriler kullanılmak suretiyle kamu kurumlarında ya da bankalarda yasal olmayan, fakat yasal gibi gösterilmeye çalışılan işlemler yapıldığını Yargıtay kararlarında tespit etmek mümkündür. İç hukuk yönünü ve bunun yansımasını yargı kararları ile takip ederken, kişisel verilerin özel hayatın gizliliğine dokunmaksızın kullanılmasının sınırını çizen uluslararası çalışmalar ve sözleşmeler ile bu sözleşmelere taraf devletlere iç hukuklarında özenli olmaları gerektiği hatırlatılmaktadır. Nitekim bu uluslararası sözleşmelerin başında AIHS ve bunun uygulama mercii AIHM gelmektedir.

I. Özel Hayatın Bir Parçası Olarak Kişisel Veri

Kişisel verilerin kullanımının sınırlarının çizilmesi, bir başka ifade ile kişisel verilerin etkin bir biçimde korunması demokratik bir toplumun gereğidir. Bu korumanın öznesi bireydir ancak bu sadece bireyin bireye karşı korunması değildir. Kişisel verilerin özel hayata müdahale teşkil edebilecek nitelikteki hukuka aykırı kullanımını ticari şirketler ve hatta devlet organları da geçekleştirebilir. Burada korunması gereken bireyin haklarıdır ve herkese karşı korunmalıdır.

[•] Galatasaray Üniversitesi Hukuk Fakültesi Ceza ve Ceza Usul Hukuku Anabilim Dalı Öğretim Üyesi

Özel hayat her yerde vardır. Kişinin sadece mahremi olarak algılanması yeterli değildir. Özel hayat, kişinin kamusal alanda bulunduğu sırada da vardır, bir suç şüphesi altında bulunan şüphelinin, yargılanan bir sanığın ya da bir mahkûmun da özel hayatı vardır. Bunlar tabii ki sınırlandırılmıştır ama dayanağı meşru ve yasal olmak zorundadır. Bu özel hayat nedir? Özel hayatın parçası olan kişisel veriden anlaşılması gereken nedir?

Özel hayat kavramı doktrinde de ifade edildiği üzere "*tanınması kolay, tanımlanması zor bir kavram"*dır[1]. Özel hayat tanımlanırken üçlü bir ayırıma gidilmekte ve bunun genel yaşam alanı, özel yaşam alanı ve sır alanından oluştuğu belirtilmektedir. Genel yaşam alanı, kişinin herkesle paylaştığı alan; özel yaşam alanı tanıdığı, söz konusu alanı paylaşmak istediği kişilere açtığı alan ve sır alanı ise sadece kendisine sakladığı alan olarak tanımlanmaktadır[2]. Özel hayatın parçaları olarak kabul edilen bu alanların hepsinde kişinin özel alanı korunmaktadır. Buradaki ayırımdaki kıstas kişinin rızasıdır.

Özel hayata müdahale olarak kabul edilen konular sadece bireylerin, diğerlerinin özel alanlarına rızaları olmaksızın girmeleri ile ortaya çıkmaz. Devlet de bu alana müdahale edebilir. Bu müdahaleye izin verildiği haller Anayasa ve ilgili Kanun ile düzenlenmiştir. Anayasa'nın 20. maddesi özel hayatın gizliliği ve korunmasını düzenlerken, bu alana hangi hal ve şartlarda müdahalenin hukuka uygun olabileceğini de belirtmektedir. Buna göre; "*Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.*

Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.

(Ek fıkra: 7/5/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda

[1] Küzeci Elif, Kişisel Verilerin Korunması, 3. Baskı, Turhan, Ankara 2019, 69.
[2] Araslı Oya, Özel Yaşamın Gizliliği Hakkı ve T.C. Anayasasında Düzenlenişi, Ankara 1979, Yayımlanmamış Doktora Tezi, nakleden Küzeci, 69-70.

öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.[3]

Anayasa'nın 20. maddesinin 2. fıkrasında özel hayatın gizliliğine ve bu kapsamda kişisel verilerin özüne ancak, millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya bir kaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamayacağını açıkça ifade eden bu hükme 2010 yılında eklenen üçüncü fıkra ile kişisel verilerin de bu kapsamda değerlendirilmesi gerektiği ifade edilmiştir.

Kişisel veri, özel hayat içinde tanımlanan bir hak olmasına rağmen, özel hayatın kapsamının çok geniş olduğu ve kişisel verilerin bu alanın sadece bir parçasını oluşturabileceği ve hatta artık bunun bağımsız bir kişilik hakkı olarak nitelendirilmesi gerektiği ifade edilmektedir. Anayasa ile 2010 yılında açıkça öngörülen kişisel veri kavramı da tıpkı özel hayat gibi tanımlanması zor bir kavramdır[4]. Kişisel veri, 6698 sayılı Kişisel Verilerin Korunması Kanunu m.3/1-d' de tanımlanmıştır. Buna göre; ***"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"*** kişisel veridir. Bu çok geniş ve belirsiz bir tanımdır. Bu tanımın içeriğini doldurmak, kişisel verinin sınırlarını çizebilmek, her türlü bilgiyi çerçevelemek oldukça zordur. Bu güçlük hem kişisel verilerin korunmasını zorlaştırmakta hem de keyfi müdahalelere açık hale getirmektedir. Bu konuda ne yazık ki uluslararası mevzuatta da yer alan tanımlar belirsizdir. OECD Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeleri; BM Evrensel İnsan Hakları Bildirgesi (m.12); BM Medeni ve Siyasal Haklar Sözleşmesi (m.17); BM'in kişisel verilerin korunması, dolaşımının engellenmesine ilişkin kabul ettiği rehber ilkeler; Avrupa Konseyi'nin temel metni AIHS'nin 8. maddesi ile Avrupa Konseyi Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi[5] gibi kişisel verilerin korunmasına yönelik uluslararası sözleşmelerle hedeflenen veri güvenliği, kişisel verilerin özel olarak korunmasıdır. Kişinin verisi de özel hayatın bir parçası olarak kabul edildiği içindir ki bu haklar çoğunlukla birlikte değerlendirilmektedir. Nitekim AIHS'nin 8. Maddesi özel hayatın gizliliğini şu şekilde

[3] Kişisel verilerin korunmasını anayasal düzeyde sağlayabilmek adına kanun koyucu 2010 tarihinde 5982 sayılı Kanun ile Anayasa'nın 20. Maddesine bu hükmü eklemiştir. (7/5/2010-5982/2 md.).
[4] Kangal Zeynel, Kişisel Verilerin Ceza Ve Kabahatler Hukukunda Korunması, Oniki Levha, İstanbul 2019, 21.
[5] Türkiye bu Sözleşme'yi 28 Ocak 1981 tarihinde imzalamış, fakat 2016 yılında onaylayarak, 29628 sayılı Resmi Gazete'de yayımlamak suretiyle iç hukukunun parçası haline getirmiştir.

tanımlamaktadır: "*1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.*

2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir". Türkiye Cumhuriyeti Anayasasında belirtilen sınırlama sebepleri AIHS'de de yer almıştır. Bu sebepler kişisel verilerin kullanımının da sınırlarını oluşturmaktadır.

II. Sınırları

Bu konuda önemli bir karar mercii olan AIHM'nin özel hayatın gizliliği kapsamında ele aldığı kişisel verilerin kullanımı ve korunmasına yönelik kararlarında belirlediği kıstaslar hem tanımları belirli hale getirmesi bakımından hem de yazılı metinlerin uygulama ile şekillenen sınırlarını tespit bakımından incelenmesi önem arz etmektedir. AIHM'nin çizdiği sınırlar nelerdir sorusuna cevap arayan ikinci bölümde bazı önemli kararlar çerçevesinde sınırları incelemeye çalışacağız. Gerek Anaysamızda (AY.m.20) gerek AIHS'de (AIHS.m.8) belirtildiği üzere özel hayatın gizliliği sınırlandırılabilir bir haktır. Bu hakkın sınırını ise yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir alınması durumu oluşturmaktadır.

Uluslararası sözleşmelerde ve Anayasa'da çerçevesi çizilen özel hayat ve kişisel verilerin korunmasına ilişkin hükümler iç hukukta uygulanabilir normlarla etkin hale getirilmiştir. Buna ilişkin en önemli düzenlemeler 5237 sayılı TCK'nın ikinci kitap kişilere karşı suçlar başlıklı ikinci kısmının özel hayata ve hayatın gizli alanına karşı suçlar başlıklı dokuzuncu bölümünde öngörülmüştür. Bu bölümde haberleşmenin gizliliği, kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması, özel hayatın gizliliği, kişisel verilerin kaydedilmesi, verilerin hukuka aykırı yayılması, hukuka uygun bir şekilde toplanmış olsa da bunların yok edilmesi gereken zamanda yok edilmemesi dolayısıyla gerçekleşen hak ihlalleri suç olarak düzenlenmiştir. Türk Ceza Kanunu ile kişisel verilerin kullanımının suç teşkil etmesi bu hakka haksız müdahalede varılacak son noktadır. Burada sınır aşılmıştır.

Kişisel verilerin kullanımının sınırları gerek uluslararası mevzuat, gerek iç hukukta yukarıda da değindiğimiz bazı düzenlemelerle çizilmiştir. Ancak bu sınırların öngörüldüğü

düzenlemeler de kişisel verinin kendisine verilen, yüklenen anlamla tespit edilmektedir. Bu konuda AIHM kararları önemli bir yol göstericidir. AIHM, AIHS ve buna bağlı ek protokollerle korunan hak ve özgürlüklerin ihlalleri karşısında yaptığı hukuki değerlendirmeler sonucu vardığı kararlarla içtihatlarını oluşturmaktadır. Bizim konumuz özelinde özel hayatın gizliliğinin unsuru olarak kişisel verilerin kullanımının sınırlarını çizen kararları da bulunmaktadır.

AIHM'nin kişisel verileri değerlendirdiği en önemli kararlarının başında Almanya'ya karşı Klass ve diğerleri kararı[6] gelmektedir. Klass içtihatı olarak nitelendireceğimiz karar kişisel verilerin kullanımının sınırlarını çizen ilk karar olma özelliğini de taşımaktadır[7]. Bu kararda demokratik bir toplumda gerekli, yasal düzenlemeye uygun ve bu düzenlemelerin de ulaşılabilir ve öngörülebilir olması gerektiğini vurgulayarak, kişisel verinin kişilik hakkı ile doğrudan bağlantılı olduğunu vurgulayarak keyfi sınırlandırılamayacağını vurgulamaktadır.

[6] Klass ve diğerleri v./Almanya, K.5029/71, T.6 Eylül 1978.
[7] Küzeci, 138.

AVRUPA İNSAN HAKLARI MAHKEMESİ KARARLARINDA İTİBARIN KORUNMASI

PROTECTION OF REPUTATION IN JUDGMENTS OF THE EUROPEAN COURT OF HUMAN RIGHTS

Dr. Ali Osman Karaoğlu

EXTENDED ABSTRACT

International law has enhanced and expanded very speedily since the second half of twentieth century. Such a similar growth has taken place in the number of international legal remedies through which individuals can sue against the state. In this sense, one of the most effective legal remedies designed to enable protection of individuals in the international law is the right to make an individual application to the European Court of Human Rights (ECtHR). However, individual application to the ECtHR is recognised as the secondary legal remedy in principle (called as the principle of subsidiarity). Accordingly, fundamental rights and freedoms shall be first safeguarded by the state, and only in case of exhaustion of domestic remedies, individuals can lodge an individual application to ECtHR. In more explicit words, in case of violation and infringment of any fundamental rights and freedoms, states are offered a chance to remedy this violation and its consequences. Nevertheless, the individuals, who are in the strong opinion that the acts of the State actually violate the rights and freedoms regulated in ECHR and that the State becomes incapable of making up for the violations, are entitled to apply to ECtHR. From this very situation, ECtHR derives its implicit role of guiding the states with respect to limits of fundamental rights and freedoms. In this context, judgments delivered by ECtHR have made remarkable contributions to human rights law.

Freedom of expression reserves a special place for democratic societies. ECtHR defines and prescribes the scope of freedom of expression in its famous *Handyside v. UK* judgment: Freedom of expression constitutes the essential foundations of both advancement of a society and development of persons. Without any prejudice to Subparagraph 2 of Article 10, this freedom is applicable not only to ‘information’ and ‘thoughts’ perceived as good or inoffensive but also for protesting, shocking and disturbing information and thoughts. Actually protection of reputation must be addressed and handled in tandem with the tension between freedom of expression and protection of private life. According to the Court in the case of *Von Hannover v. Germany,* the private life encompasses all aspects of one’s personality inclusive of one’s name, image, its written works or identity. This indicates that private life covers psychological integrity of a person as well as the physical one.

Driven by the growth in the means of mass communication such as media and internet, the content and scope of classical rights have been expanded to such extent that it has been required to address each of them seperately and respectively, as seen in the instance of protection of reputation in the international human rights law. In this regard, protection of reputation has not been regulated as a distinct human right in international treaties, instead, it has been asssured in the Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and Article 8 of the European Convention on Human Rights (ECHR) entitled as “right to respect for private

and family life". On the other hand, protection of reputation has been mentioned as "the protection of the reputation or rights of others" amonst the limits of Article 10 of the ECHR entitled "freedom of expression". European Court of Human Rights (ECtHR) paid special attention to protection of reputation and exerted efforts to establish fair balance between freedom of expression and protection of reputation in its judgments.

When protection of reputation is concerned, ECtHR has identified some criteria as to how to maintain a fair balance between protection of private life and freedom of expression. In its landmark judgment *Axel Springer v. Germany*, ECtHR rules that a fair balance is required to be established between private life and freedom of expression in light of such criteria as contribution to a debate of general interest, how well known is the person concerned; prior conduct of the person concerned; method of obtaining the information and its veracity; content, form and consequences of the publication; severity of the sanction imposed. On the other hand, the principles generally applied in its judgments pertaining other rights such as margin of appreciation, necessity in democratic society and proportionality have been similarly applied by the ECtHR to setting up of a fair balance between freedom of expression and protection of reputation. This study aims to examine scope and limits of the right to protection of reputation which is often featured in debates and to further analyze how fair balance is established between freedom of expression and protection of reputation in the judgments of the ECtHR.

1. Giriş

Uluslararası hukuk, özellikle, 20. yüzyılda bireyleri de koruma altına almaya başlamış ve 1945 sonrası gelişmeler uluslararası insan hakları hukukunun olağanüstü düzeyde genişlemesine neden olmuştur. Nitekim devletler sadece otuz yıl içerisinde yaşanan iki büyük savaşın etkisi ile evrensel ve bölgesel anlamda insan hakları andlaşmaları akdetmeye başlamış ve birtakım koruma mekanizmaları oluşturmaya çalışmıştır. Bu anlamda evrensel mekanizmalar BM bünyesinde kurulduysa da en etkin koruma mekanizması Avrupa sisteminden neşet etmiştir. Nitekim Avrupa Konseyi bünyesinde toplanan devletler Avrupa İnsan Hakları Sözleşmesi'ni (AİHS) akdetmiş ve sözleşmede yer alan temel hakların korunması için Avrupa İnsan Hakları Mahkemesi'ni (AİHM) kurmuştur.[1] Ancak AİHM'e bireysel başvuru kural olarak ikincil bir hukuk yoludur (principle of subsidiarity). Buna göre temel hak ve özgürlükler öncelikle devlet tarafından korunacak ancak bireyler ancak iç hukuk yollarını tükettikten sonra (exhaustion of domestic remedies) AİHM'e bireysel başvuruda bulunabileceklerdir. Daha açık ifade ile temel hak ve özgürlüklerin ihlali durumunda öncelikle devlete bu ihlali ve neticelerini giderme imkanı verilir. Devletin eyleminin AİHS'te düzenlenen hak ve özgürlükleri ihlal ettiğini ve devletin ihlali gidermede yetersiz kaldığını düşünen bireyler AİHM'e başvurabilir. [2] Bu durum da AİHM'e; sözleşmede düzenlenen temel hak ve özgürlüklerin sınırları konusunda devletlere, zımni olarak, yol gösterme imkanı verir.[3]

---

[1] Luzius Wildhaber, 'The European Court of Human Rights: The Past, The Present, The Future' American University International Law Review, Vol. 22, No. 4 (2007), s.522-23.

[2] Marisa Iglesias Vila, 'Subsidiarity, Margin of Appreciation and International Adjudication Within a Cooperative Conception of Human Rights', International Journal of Constitutional Law, Volume 15, Issue 2, April (2017), s.401.

[3] İtibarın, şeref ve haysiyetin veya kişilik haklarının korunması Türk hukukunda da çeşitli kanunlar tarafından koruma altına alınmıştır. Türk hukukunda itibarın korunmasına ilişkin davalarda AİHM'den önce son karar mercii Türk Anayasa Mahkemesi (AYM)'dir. İfade özgürlüğü ile itibarın korunması arasındaki denge AYM kararlarında da değerlendirilmekte ve temel itibariyle uyuşmazlığa uygulanacak uluslararası hukuk açısından AİHM kararlarına atıf yapılmaktadır. Bu anlamda örnek bir karar için bakınız: AYM, Ali Kıdık Başvurusu, Başvuru Numarası:

Teknoloji ve kitle iletişim araçlarının gelişmesi uluslararası hukukun koruması altında olan temel hak ve özgürlüklerin kapsamını genişletmektedir. Bu anlamda artık internet ve sosyal medya gibi araçlar özelinde çalışmalar yapılmakta ve klasik koruma kapsamına bu tür mecralarda gerçekleşen eylemler de eklenmektedir. Bu durumun bir neticesi olarak itibarın korunması hakkı teknoloji geçtikçe önemini arttırmaktadır. Esas itibariyle itibarın korunması AİHS'in 10/2. maddesinde düzenlenen "ifade özgürlüğü"nün sınırlarından birini teşkil etmektedir. Buna göre ifade özgürlüğü "başkalarının şöhret ve haklarının korunması için gerekli olan bazı formaliteler, koşullar, sınırlamalar veya yaptırımlara tabi tutulabilir".[4] Madde düzenlemesine göre itibarın korunması, ifade özgürlüğünün kısıtlanması için kullanılabilecek bir meşru amaçtır. Öte yandan itibarın korunması AİHS'in 8. maddesinin de koruması kapsamına girmektedir. "Özel hayata ve aile hayatına saygı hakkı" başlığını taşıyan 8. maddenin 1. fıkrasına göre: "Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir".[5] Bu anlamda bireyin itibarı da özel hayat kapsamında sayılmakta ve itibarın karalanması 8. maddenin ihlali olarak kabul edilmektedir. Bu anlamda ifade özgürlüğü ile özel hayatın korunması arasındaki adil dengenin nasıl kurulacağı da AİHM kararlarında ele alınmıştır. Çalışmamız da AİHM kararları ışığında itibarın korunması özelinde ortaya konan kriterleri inceleyecek ve mümkün olduğu kadar uluslararası insan hakları hukuku çerçevesi içerisinde kalacaktır.

2. AİHM Kararlarında İtibarın Korunması

İfade özgürlüğü demokratik toplumlar açısından özel bir yere sahiptir. Nitekim AİHM meşhur *Handyside v. UK* kararında ifade özgürlüğü'nün kapsamını şu şekilde belirlemiştir: "İfade özgürlüğü, demokratik bir toplumun ilerlemesinin ve kişilerin gelişiminin temel esaslarından birini oluşturmaktadır. 10. maddenin 2. bendi saklı kalmak kaydıyla, bu özgürlük, sadece, iyi algılanan veya zedeleyici olmayan 'bilgi' ve 'düşünceler' için değil, aynı zamanda, çatışan, şaşırtan veya endişelendiren bilgi ve düşünceler için de geçerlidir".[6] İtibarın korunması esas itibariyle ifade özgürlüğü ve özel hayatın korunması arasındaki gerilim ile birlikte ele alınmalıdır. *Von Hannover v. Germany* davasında Mahkemeye göre özel hayat kişinin adı, fotoğrafı, yazdığı yazılar veya kimliği gibi kişiliğe ait tüm yönleri içerisine alır. Bu anlamda özel hayat kişinin fiziksel bütünlüğünün yanında psikolojik bütünlüğünü de kapsar.[7] Mahkemenin bu anlamda ifade özgürlüğü ve özel hayat arasındaki adil dengeyi nasıl kurduğu önem arz etmektedir.

2.1. Tanınmış Kimseler ve Siyasiler Açısından İtibarın Korunması

İtibarın korunması açısından AİHM özel hayatın korunması ile ifade özgürlüğü arasındaki adil dengenin nasıl kurulacağına dair birtakım kriterler belirlemiştir. Bu kriterlerin kapsamlı bir şekilde oluşturulduğu en meşhur karar olan *Axel Springer v. Germany* davasına konu olan olayda Axel Springer, Almanya'da yerleşik ve Bild gazetesinin sahibi olan bir şirkettir. Bild gazetesi Almanya'da meşhur bir aktör olan X hakkında farklı zamanlarda iki makale ve bazı görüntüler yayınlamıştır. Makalelere göre X hakkında Münih'te düzenlenen Oktoberfest adlı

2014/5552, Karar Tarihi: 26/10/2017, R.G. Tarih ve Sayı: 14/12/2017 – 30270, parag.22 vd. Çalışmamız ise yalnızca AİHM kararlarına odaklanacaktır.

[4] Avrupa İnsan Hakları Sözleşmesi, madde 10/2. https://www.echr.coe.int/Documents/Convention_TUR.pdf (erişim tarihi: 19.10.2019).

[5] Avrupa İnsan Hakları Sözleşmesi, madde 8/1.

[6] Handyside v. United Kingdom, Application no. 5493/72, Judgment, 7 December 1976, parag.49.

[7] Von Hannover v. Germany, Application no. 59320/00, Judgment, 24 June 2004, parag.50.

festivalde kokain içtiği gerekçesiyle savcılık tarafından işlem başlatılmış ve neticede tutuklanmıştır. Bild gazetesinin yayınladığı bilgilere göre yargılama neticesinde X para cezasına çarptırılmıştır. Bunun yanısıra X'e ait bazı fotoğraflar da yayınlanmıştır. Öte yandan X her iki makalenin ve fotoğrafların kişilik haklarına saldırı olduğu ve itibarını zedelediği gerekçesiyle mahkemeye başvurmuş ve Alman mahkemeleri tarafından makalelerin yasaklanması yönünde karar verilmiştir. Mevzubahis kararlar ayrıca üst mahkemelere de taşınmış ve onanmıştır. Axel Springer böylece iç hukuk yollarını tükettikten sonra ifade özgürlüğünün ihlal edildiği gerekçesi ile AİHM'e başvurmuştur.[8] Mahkeme ise ifade özgürlüğünün ihlal edildiği yönünde karar vermiştir. AİHM'e göre kamu yararına dair genel bir tartışmaya katkı, uyuşmazlığa konu kimsenin ne kadar tanındığı, kişinin daha önceki davranışları, bilgiyi elde etme şekli ve bilginin doğruluğu, bilginin içeriği ve hangi şekilde yayınlandığı, uygulanan yaptırımın ağırlığı gibi kriterlere bakılarak ifade özgürlüğü ile özel hayat arasında adil bir denge kurmak gerekir.[9] Somut olayda basında yer alan ifadelerin kısıtlanması demokratik toplum açısından gerekli görülemez. Mahkeme çeşitli kararlarında bu kriterleri başkaca olaylara uygulamış itibarın korunması hakkında yerleşik bir içtihat oluşturmaya çalışmıştır. *Egill Einarsson v. Iceland* davasında başvurucu İzlanda'da meşhur bir karakter olup hakkında açılan tecavüz soruşturması Savcılık tarafından delil yetersizliğinden devam ettirilmemiştir. Başvurucunun röportaj verdiği ve fotoğrafının bulunduğu bir derginin kapağı bir Instagram kullanıcısı tarafından değiştirilerek "tecavüzcü" ve başkaca argo kelimeler ile birlikte Instagram'da yayınlanmıştır. AİHM tanınmış kişi dahi olsa açıkça dayanaktan yoksun bir şekilde bu kimseler hakkında ağır bir suçu işlediği vehmini uyandıracak kişilik saldırılarının tolere edilemeyeceğini ifade ederek 8. maddede belirtilen özel hayatın (itibarın) ihlal edildiğine karar vermiştir.[10]

AİHM tanınmış kişiler arasında özellikle siyasilerin özel hayatlarının korunması açısından daha esnek bir koruma öngörmekte ve siyasilerin bu anlamda daha tahammüllü olması gerektiğini düşünmektedir. Zira siyasilerin özel hayatı kamusal faaliyetlerinin yürütülmesini etkileyebilecek niteliktedir. *Lingens v. Austria* davasına konu olayda Lingens seçimleri kazanan Avusturya Şansölyesini eleştiren yazılar yayınlamıştır. Lingens'e göre Şansölye'nin koalisyon ilan ettiği partinin başkanı Nazi kökenli bir kimsedir. Bu anlamda Lingens, Şansölye'nin siyasi girişimini haysiyetsizlik ve Nazi hareketini devam ettirme girişimi olarak nitelendirmiştir. Şansölye ise Lingens hakkında dava açmış ve yapılan yargılamalar neticesinde Lingens, sözlerinin hakaret niteliğinde olduğu ve dolayısıyla itibarın zedelendiği gerekçesiyle para cezasına çarptırılmıştır. Dava ifade özgürlüğünün ihlal edildiğinden bahisle AİHM önüne taşınmıştır. Mahkemeye göre demokratik toplumlarda basın yoluyla ifade özgürlüğü özel bir önem taşımaktadır. Zira toplum basın sayesinde siyasilerin fikir ve tutumları konusunda bilgilenmekte ve kanaatini oluşturmaktadır. Bu anlamda siyasi meseleleri tartışma özgürlüğü demokratik toplumun temel bileşenlerindendir. Siyasiler bilinçli bir şekilde tüm sözlerini kamuoyunun incelemesine açmaktadır. Elbette ki siyasilere yönelecek eleştirinin sınırları sıradan insanlara göre daha geniş kabul edilecek ve siyasilerden daha fazla hoşgörülü olmaları beklenecektir. Mahkeme bu anlamda siyasilerin de itibarının koruma altında olduğunu

[8] Axel Springer AG v. Germany, Application no. 39954/08, Judgment, 7 February 2012, parag.9-12.
[9] Axel Springer AG v. Germany, parag.90-95. Dominika Bychawska-Siniarska, 'Protecting the Right to Freedom of Expression under the European Convention on Human Rights', Council of Europe Publications, July (2017), s.63.
[10] Egill Einarsson v. Iceland, Application no. 24703/15, Judgment, 7 November 2017, parag.52.

belirtmekle birlikte bu korumayı demokratik toplum menfaatleri ile birlikte ele almıştır.[11] Öte yandan Mahkeme *Sanocki v. Poland* kararında gerçek olmayan, kamuyu yanıltıcı haber ve bilgiler söz konusu olduğunda siyasilerin itibarının korunması gerektiğine de vurgu yapmıştır.[12]

Mahkeme kamu görevlilerine yönelen ve kamuyu ilgilendiren eleştiriler konusunda da itibarın korunmasını geniş bir şekilde ele almaktadır. *Thorgeirson v. Iceland* davasına konu olayda başvurucu günlük bir gazetede polis şiddeti üzerine birtakım yazılar yayınlamıştır. Başvurucu polis teşkilatı içerisindeki şiddetin toplumdan gizlendiğini, polisler arasında "üniformalı hayvanların" bulunduğunu, kabadayılık ve sahtekarlığın gittikçe arttığını iddia etmiştir. Yazar polis memurlarının itibarını zedelediği gerekçesiyle para cezasına mahkum edilmiş ve uyuşmazlık AİHM'e taşınmıştır. Mahkeme'ye göre basın bir nevi "kamusal bekçi köpeği" (public watchdog) görevi görmekte, basın sayesinde toplum kamuya ilişkin meseleleri tartışabilmektedir. Bu anlamda itibarın korunmasına dayanarak ifade özgürlüğünün kısıtlanması, toplumda kamusal meseleleri tartışma noktasında bir çekingenliğe neden olacaktır. Kullanılan ifadelerin sertliği ifade özgürlüğünün kısıtlanması için tek başına yeterli neden oluşturmaz.[13] Öte yandan *Thoma v. Luxembourg* davasında Mahkemeye göre; resmi sıfatla hareket eden kamu görevlileri de eleştiri bakımından siyasetçiler gibi geniş sınırlara tabidirler. Ancak kamu görevlilerinin bilerek her eylemini de kamusal tartışmaya açtıkları da söylenemez.[14] Bu anlamda esasen Mahkeme kamu görevlileri açısından da ifade özgürlüğünün kapsamını genişletmekle birlikte konuyu siyasiler düzeyinde de değerlendirmemektedir. *Kaboğlu and Oran v. Turkey* davasında Mahkeme, insan hakları konusunda danışmanlık yapmak üzere atanan üniversite profesörlerinin politikacılar gibi düşünülemeyeceğini ve bu kimselere karşı yöneltilen kişilik hakkı saldırılarının daha dar yorumlanması gerektiğini vurgulamıştır.[15]

Olafsson v. Iceland davasında Pressan isimli bir online sitenin editörü birtakım makaleler yayınlayarak bir politikacının çocukların cinsel istismarı suçunu işlediğine dair üstü kapalı göndermelerde bulunmuştur. İzlanda Mahkemeleri editörü, politikacının karalanması (defamation) ve itibarının zedelenmesinden bahisle mahkum etmiştir. Dava ifade özgürlüğünün ihlali gerekçesiyle AİHM'e taşınmıştır. Mahkeme ifade özgürlüğü ile özel hayat ve itibarın korunması arasındaki adil dengenin kurulamadığını belirtmiş ve ifade özgürlüğünün ihlal edildiğine karar vermiştir. Mahkeme'ye göre bir politikacı hakkında toplumun değerlendirmesini gerektirecek böylesi bir iddianın tartışmaya açılmasında bir beis yoktur. Üstelik tartışma olağan basın standartları kapsamında ortaya çıkarılmıştır. Zira politikacı hakkındaki iddialar daha önceki tarihlerde aile arasında ve çeşitli mecralarda erişilebilir şekilde tartışılmıştır. Pressan'ın yaptığı bu iddiaları derlemek mahiyetindedir. Bu tür bir ifadenin kısıtlanması için demokratik toplum açısından gereklilik söz konusu değildir.[16] Öte yandan *Standard Verlags v. Austria* davasına konu olan olayda şirketin sahip olduğu gazetelerden birinde Avusturya Başkanı hakkında çeşitli iddialara yer verilmiştir. Buna göre gazetede başkanın eşinin boşanmak istediğine yer verilmiş ve boşanmanın gerekçesi olarak da başkanın iki erkek ile (Avusturyalı bir politikacı ve yabancı bir büyükelçi) ilişkisi olduğu ileri

[11] Lingens v. Austria, Application no. 9815/82, Judgment, 8 July 1986, parag.42.
[12] Sanocki v. Poland, Application no. 28949/03, Judgment, 17 July 2007, parag.61.
[13] Thorgeirson v. Iceland, Application no. 13778/88, Judgment, 25 June 1992, parag.63-70.
[14] Thoma v. Luxembourg, Application no. 38432/97, Judgment, 29 March 2001, parag.47.
[15] Kaboğlu and Oran v. Turkey, Application no. 1759/08, 50766/10 and 50782/10, Judgment, 30 October 2018, parag.74.
[16] Olafsson v. Iceland, Application no. 58493/13, Judgment, 16 March 2017, parag.49-62.

sürülmüştür. Bunun üzerine gazetenin sahibi karalama ve iftira suçundan mahkum edilmiştir. Dava AİHM'e taşınmış ve Mahkeme ifade özgürlüğünün ihlalinin söz konusu olmadığına karar vermiştir. Mahkemeye göre kişilerin özel hayatları ve itibarı hakkında asılsız dedikodu yayma karşısında ifade özgürlüğünün korunması söz konusu olamaz. Böyle durumlarda kişiler itibarının korunması demokratik toplumda gereklidir. Bu anlamda somut olayda başvurucunun mahkum edilmesi ölçülülük ilkesi ile çelişmez.[17]

2.2. Ticari İtibar ve Toplum Yararı

AİHM ticari şirketlerin itibarını gerçek kişilerin itibarından ayrı tutmaktadır. *Kulis and Roziycki v. Poland* davasına konu olayda patates cipsi üreticisi bir firma, reklamlarında çocuklar için popüler bir çizgi film karakteri olan Reksio'yu "katil" olarak çağıran ifadelere yer vermiştir. Başvurucuya ait derginin çocuk eki de bir karikatür yayınlayarak bu reklama tepki göstermiştir. Başvuruculların derginin ön kapağında yayınladıkları karikatürde elinde firmanın ismini taşıyan patates cipsi taşıyan bir çocuk "endişelenme! bu pisliği yeseydim ben de katil olurdum" demektedir. Karikatürün yayınlandığı sayfanın manşetinde ise "Polonyalı çocuklar cips reklamı ile şok oldu: Reksio bir katil" yazısı yer almaktaydı. Bunun üzerine firma ticari itibarının ve haklarının zedelendiğinden bahisle yerel mahkemeler önünde dava açmış ve davası kabul edilmiştir. Daha sonra iç hukuk yollarını tüketen başvurucu uyuşmazlığı AİHM'e taşımıştır. Mahkeme esasen kullanılan sözlerin ağır olduğunu tespit etmekle birlikte yayımlanan karikatürün firmayı zarara uğratmak amacıyla yayımlanmadığını, firmanın şoke edici reklamını eleştiri amacıyla yayımlandığını vurgulamıştır. Nitekim bu amaç manşet yazısından da anlaşılmaktadır. Mahkemeye göre küçüklerin çok sevdiği bir çizgi film karakterinin bu şekilde reklamlarda kullanılması onların ruhsal durumlarına zarar verebilir ve bu anlamda ortaya korunması gereken bir toplum yararı ortaya çıkar. Bu nedenle böyle bir karikatürün yayımlanması üzerine ifade özgürlüğünün kısıtlanması ihlal teşkil eder.[18] *Uj v. Hungary* davasına konu olayda başvurucu Peter Uj yayınladığı bir yazıda bir devlet şirketi olan ZRT'nin ürettiği birayı "dışkı" şeklinde nitelemiş ve kalitesini sert bir dille eleştirmiştir. ZRT şirketinin ticari itibarının karalandığı gerekçesiyle Macaristan mahkemelerine başvurmuş ve Uj mahkum edilmiştir. Bunun üzerine dava ifade özgürlüğünün ihlal edildiğinden bahisle AİHM'e taşınmıştır. Mahkeme ifade özgürlüğünün kısıtlanması için yeterli gerekçenin bulunmadığını tespit ederek ihlal yönünde karar vermiştir. Mahkeme gerçek kişiler ile ticari şirketlerin itibarı arasında bir fark olduğunu ve ticari şirketlerin itibarının ahlaki boyuttan düşünülemeyeceğini belirtmiştir. Gerçek kişilerin çevresi nezdinde sosyal kimliği veya onuru zedelenebilirken ticari şirketlerde bu tür şeyler görülmeyebilir. Mahkeme esasen ifadelerin abartılı ve provokatif olsa dahi bir toplumsal tartışmaya ilişkin olduğunu ifade etmiştir. Buna göre başvurucu esasen devletin sahibi olduğu şirketlerin ürettiği ürünler ile özel ya da yabancı şirketlerin ürettiği ürünler arasında fark olduğunu belirtmiş ve devlet şirketlerinin bu anlamda dezavantaj yarattığını anlatmaya çalışmıştır.[19]

2.3. Mahkemeler ve Yargı Mensuplarının İtibarı

Toplumlar açısından adalete ve yargının tarafsızlığına olan güvenin sarsılmaması için yargı kurumları ile hakimler ve savcılar gibi yargı mensuplarının da itibarının korunması gerekir. Ancak bu durumda da eleştiri içerikli ifade özgürlüğü ile yargının itibarının korunması arasında

[17] Standard Verlags GmbH v. Austria, Application no. 21277/05, Judgment, 4 June 2009, parag.53-56.
[18] Kuliś and Różycki v. Poland, Application no. 27209/03, Judgment, 6 October 2009, parag.37-40.
[19] Uj v. Hungary, Application no. 23954/10, Judgment, 19 July 2011, parag.22-26.

bir dengenin kurulması şarttır. Bu anlamda *The Sunday Times v. UK* kararında AİHM; mahkemelerin bir boşluk (vacuum) içerisinde faaliyet gösteremeyeceğine dair genel bir kanaatin var olduğunu, mahkemelerin uyuşmazlıkları çözmesinden önce kamuyu ilgilendiren tartışmaların yapılabileceğini ve bunun da en iyi bir şekilde basın tarafından dile getirilebileceğini vurgulamıştır.[20] Hakimlerin itibarının korunması açısından Türkiye'ye karşı açılmış birkaç dava vardır. *Mustafa Erdoğan v. Turkey* davasına konu olayda Anayasa Hukuku profesörü olan olan başvurucu 2001 yılında Fazilet Partisi'nin Anayasa Mahkemesi (AYM) tarafından kapatılması üzerine yazdığı bir makalede bazı AYM üyelerini eleştirmiş ve kendilerinin ne demokrasi ne de siyasetten anladıklarını, entelektüel kapasitelerinin yetersiz olduğunu belirterek statükonun savunuculuğunu yaptıklarını beyan etmiştir.[21] Bunun üzerine AYM üyeleri kişilik haklarına saldırı ve itibarın zedelenmesinden bahisle Türk mahkemeleri nezdinde dava açmış ve Mustafa Erdoğan tazminata mahkum edilmiştir. Daha sonra dava ifade özgürlüğünün ihlal edildiğinden bahisle AİHM'e taşınmıştır. Mahkeme Axel Springer davasında tartıştığı kriterler bağlamında ifade özgürlüğü ve itibarın korunması hakkında adil bir denge kurmaya çalışmıştır.[22] Mahkeme; uyuşmazlığa konu olan ifadelerin güncel ve kamuyu ilgilendiren bir mesele hakkında sarf edildiğini, akademisyenlerin kendi uzmanlık alanları ile ilgili görüşlerini paylaşmasının olağan olduğunu, hakaret ile eleştirinin birbirinden farklı olduğunu ve mahkeme üyelerinin de eleştirilebileceğini belirterek ifade özgürlüğünün demokratik toplum gerekliliklerine aykırı bir şekilde ihlal edildiğini vurgulamıştır.[23] *Poyraz v. Turkey* davasına konu olayda başvurucu adalet bakanlığı müfettişi olup bir yüksek mahkeme hakiminin soruşturulması kapsamında rapor hazırlamıştır. Raporda hakimin çeşitli cinsel istismar olaylarına karıştığı çeşitli tanık beyanları ile sert bir şekilde dile getirilmiştir. Daha sonra rapor basına sızınca ve müfettiş hakkında politik bir komploya karıştığı iddiaları gündeme gelince başvurucu bir basın açıklaması yayınlamış ve rapora konu olan hakimin on beş ayrı soruşturma kapsamında sorgulandığını beyan etmiştir. Soruşturmaya konu hakim tarafından kişilik haklarının ve itibarının zedelendiği gerekçesiyle dava açılmış ve kabul edilmiş, üst mahkemelerce de onanmıştır. İfade özgürlüğünün ihlalinden bahisle AİHM'e taşınan davada Mahkeme somut olayda başkalarının hakları ve itibarının korunması amacıyla ifade özgürlüğünün kısıtlanmasını haklı bulmuş ve ihlal görmemiştir. Mahkemeye göre kamusal sorumluluk verilen kimseler basına bilgi verirken sıradan vatandaşlara göre daha özenli olmalıdırlar. Başvurucunun beyanları basına sızan ve hakimin özel hayatı hakkındaki bilgileri teyit eder niteliktedir.[24] AİHM esasen itibarın korunmasını kişinin sosyal konumu, görevi, tanınırlığı veya siyasi pozisyonu gibi esaslar çerçevesinde değerlendirmekte ve Axel Springer kararında zikrettiği kriterleri katı bir şekilde uygulamamaktadır.

3. Sonuç

İnsan hakları hukuku teorisinde ifade özgürlüğü en temel haklardan biri olmakla birlikte mutlak (absolute) bir karaktere de sahip değildir. Bu anlamda AİHS ifade özgürlüğünü düzenlerken bazı sınırlamalar öngörmüştür. Bu sınırlamalardan bir tanesi de 8. Maddede düzenlenen başka

[20] The Sunday Times v. United Kingdom, Application no. 6538/74, Judgment, 26 April 1979, parag.65.
[21] Mustafa Erdoğan, 'Fazilet Partisi'ni Kapatma Kararı Işığında Türkiye'nin Anayasa Mahkemesi Sorunu' Liberal Düşünce, Yaz (2001), s.38-40.
[22] Mehmet Özalp, 'Avrupa İnsan Hakları Mahkemesi ve Yargıtay Kararları Işığında Türkiye'de İfade Özgürlüğü' Yüksek Lisans Tezi, ÇOMÜ Sosyal Bilimler Enstitüsü, (2016), s.125-130.
[23] Mustafa Erdoğan and Others v. Turkey, Application no. 346/04 and 39779/04, Judgment, 27 May 2014, parag.41-46.
[24] Poyraz v. Turkey, Application no. 15966/06, Judgment, 7 December 2010, parag.68-79.

bir hakkın da kapsamına giren "itibarın korunması"dır. Ancak sınırlamanın nasıl olacağı veya sınırlamanın sınırlarının nasıl saptanacağı uygulamada AİHM kararları ile ortaya konmaktadır. İfade özgürlüğü ve itibarın korunması arasında kurulacak adil denge bağlamında AİHM çeşitli kararlarında bazı kriterler oluşturmuş ve sıradan kişiler ile belirli özelliğe sahip kişiler arasında bir ayrım yapmıştır. Ayrıca kişileri de somut anlamda aynı neticeye tabi tutmamış, ifadeye konu olan bilginin gerçekliği, uygulanan yaptırımın ağırlığı, ifadenin kamu yararına matuf bir tartışmaya katkı sağlayıp sağlamadığı gibi destekleyici ölçütler ışığında her olayı kendi bağlamı içerisinde incelemiştir. Öte yandan AİHM diğer haklara ilişkin kararlarında da genel olarak uyguladığı takdir marjı (margin of appreciation), demokratik toplumda gereklilik (necessity in democratic society) ve ölçülülük (proportionality) gibi ilkeleri ifade özgürlüğü ve itibarın korunması arasındaki adil dengeyi kurarken de uygulamıştır. AİHM kararlarına genel olarak bakıldığında ifade özgürlüğü ile itibarın korunması arasındaki çatışmanın en çok ortaya çıktığı alanın basında, sosyal medyada ve online mecralarda ortaya çıkan haberler veya görüşler olduğu görülmektedir. Teknolojinin yaygınlaşması ile birlikte kitle iletişim araçlarına ulaşımın kolay hale getirmiştir. Bu durum da kişilerin itibarını zedeleyebilecek ifadelerin daha hızlı bir şekilde tedavüle sokulmasını beraberinde getirmiştir. Bu durum da esasen itibarın korunması ile ilgili olarak gelecekte AİHM'in daha çok dava yükü ile meşgul olacağını göstermektedir. Böylece insan hakları hukuku genişlemeye devam etmekte ve uluslararası hukuk kişilerin hayatını doğrudan etkileyen bir hukuk dalı olma özelliğini arttırmaktadır.

Referanslar

Avrupa İnsan Hakları Sözleşmesi, madde 10/2. https://www.echr.coe.int/Documents/Convention_TUR.pdf (erişim tarihi: 19.10.2019).

Axel Springer AG v. Germany, Application no. 39954/08, Judgment, 7 February 2012, parag.9-12.

AYM, Ali Kıdık Başvurusu, Başvuru Numarası: 2014/5552, Karar Tarihi: 26/10/2017, R.G. Tarih ve Sayı: 14/12/2017 – 30270, parag.22 vd.

Dominika Bychawska-Siniarska, 'Protecting the Right to Freedom of Expression under the European Convention on Human Rights', Council of Europe Publications, July (2017), s.63.

Egill Einarsson v. Iceland, Application no. 24703/15, Judgment, 7 November 2017, parag.52.

Handyside v. United Kingdom, Application no. 5493/72, Judgment, 7 December 1976, parag.49.

Kaboğlu and Oran v. Turkey, Application no. 1759/08, 50766/10 and 50782/10, Judgment, 30 October 2018, parag.74.

Kuliś and Różycki v. Poland, Application no. 27209/03, Judgment, 6 October 2009, parag.37-40.

Lingens v. Austria, Application no. 9815/82, Judgment, 8 July 1986, parag.42.

Luzius Wildhaber, 'The European Court of Human Rights: The Past, The Present, The Future' American University International Law Review, Vol. 22, No. 4 (2007), s.522-23.

Marisa Iglesias Vila, ‘Subsidiarity, Margin of Appreciation and International Adjudication Within a Cooperative Conception of Human Rights’, International Journal of Constitutional Law, Volume 15, Issue 2, April (2017), s.401.

Mehmet Özalp, ‘Avrupa İnsan Hakları Mahkemesi ve Yargıtay Kararları Işığında Türkiye’de İfade Özgürlüğü’ Yüksek Lisans Tezi, ÇOMÜ Sosyal Bilimler Enstitüsü, (2016), s.125-130.

Mustafa Erdoğan and Others v. Turkey, Application no. 346/04 and 39779/04, Judgment, 27 May 2014, parag.41-46.

Mustafa Erdoğan, ‘Fazilet Partisi’ni Kapatma Kararı Işığında Türkiye’nin Anayasa Mahkemesi Sorunu’ Liberal Düşünce, Yaz (2001), s.38-40.

Olafsson v. Iceland, Application no. 58493/13, Judgment, 16 March 2017, parag.49-62.

Poyraz v. Turkey, Application no. 15966/06, Judgment, 7 December 2010, parag.68-79.

Sanocki v. Poland, Application no. 28949/03, Judgment, 17 July 2007, parag.61.

Standard Verlags GmbH v. Austria, Application no. 21277/05, Judgment, 4 June 2009, parag.53-56.

The Sunday Times v. United Kingdom, Application no. 6538/74, Judgment, 26 April 1979, parag.65.

Thoma v. Luxembourg, Application no. 38432/97, Judgment, 29 March 2001, parag.47.

Thorgeirson v. Iceland, Application no. 13778/88, Judgment, 25 June 1992, parag.63-70.

Uj v. Hungary, Application no. 23954/10, Judgment, 19 July 2011, parag.22-26.

Von Hannover v. Germany, Application no. 59320/00, Judgment, 24 June 2004, parag.50.

Otonomlaştırılmış Araçlarda Veri Sorumlusu

The data controller in the autonomized motor vehicles

Ar. Gör. Dr. Cüneyt PEKMEZ

Otonomlaştırılmış araçlar, sürüşü gerçekleştirebilmek için çeşitli verilere ihtiyaç duyar. Oldukça yüklü miktarda veri toplama potansiyeli olan otonomlaştırılmış araçların sensörler, kameralar, lazerler vb. çeşitli araçlarla topladığı veriler, çeşitli veri kategorileri içerisinde incelenebilir. Bu kapsamda araca, araç içerisindeki kişilere ve araç dışındaki çevreye ilişkin olmak üzere üç kategori veriden bahsedilebilir[1].

Araçla ilgili veriler, genellikle araca ait temel bilgileri, aracın pozisyonu ve aracın durumuna ilişkin verileri kapsar. Araç içerisindeki kişilere ilişkin veriler ise, araç içerisindeki kişi (ler)in fiziki ve psikolojik durumu, kişilerin tanımlanmasına ilişkin veriler (, kişilerin tercihine ilişkin veriler, kişinin davranışına ilişkin veriler, sağlık durumuna ilişkin verilerden oluşabilir. Araç dışındaki çevreye ilişkin veriler ise, karayolu içinde ve dışındaki nesne, kişi ve araçlara, yol, trafik ve hava durumuna ilişkin verilerdir[2].

Otonomlaştırılmış araçların elde ettiği veya edeceği bu veriler, sürüş tekniğinin geliştirilmesi, sürüş ve trafik güvenliğinin sağlanması, trafiğin denetlenmesi ve sözleşmelerin ifası (sigorta, araç kirası, leasing, işveren-işçi ilişkileri) amaçlarıyla kullanılabilir. Genel itibariyle, sayılanlarla sınırlı olmamak ve her bir somut olayın özelliğine göre değişebilmekle birlikte, bu verilere, araç üreticisinin, işletenin, trafiğe katılanların, kamu kurum ve kuruluşları ile yetkili kamu görevlilerinin, sigorta şirketlerinin, araç bakım servislerinin hatta işverenlerin ihtiyaç duyabileceği söylenebilir[3].

Kişisel Verilerin Korunması Kanunu (KVKK) md. 3 (ı)'de veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi şeklinde tanımlanmıştır. Her bir somut

---

1 Barbara Widmer, "**Das vernetzte Automobil und der Datenschutz I.- IV**", Strassenverkehrsrecht – Tagung 21.- 22. Juni 2016 (Ed. Thomas Probst/Franz Werro), Stämpli, Bern, 2016, s. 143-166 (s. 150); Marit Hansen, "**Das Netz im Auto & das Auto im Netz**" Datenschutz und Datensicherheit(DuD) 2015/6, s. 367-371 (s. 367 vd.); Judith Klink-Straub/ Tobias Straub, "**Nachste Ausfahrt DS-GVO-Datenschutzrechtliche Herausforderungen beim automatisierten Fahren"**, NJW 2018, s. 3201 vd.

2 Verilere ilişkin bu sınıflandırma için bkz. **Widmer**, s. 150-151; **Hansen**, s. 368.

3 **Widmer**, s. 151-152; **Hansen**, s. 369; Astrid Auer-Reinsdorff/ Isabell Conrad, **Handbuch IT- und Datenschutz**, 3. Auf. Beck, 2019, §34 N. 879; aynı şekilde sürücünün de, otonomlaştırılmış aracın sunduğu hizmetler çerçevesinde kişisel verileri işleyebilme imkanı olduğu sürece veri sorumlusu olabileceği gözardı edilmemelidir. Ancak sistem sürücüye kişisel verileri işleme imkanı vermezse sürücü veri sorumlusu sıfatına sahip olmayacaktır. Bkz. **Hansen**, s. 369.

olayın özelliğine göre değişebileceği gözönüne alınmak ve sayılanlarla sınırlı olmamak üzere araç üreticisi, işleten, trafiğe katılanlar, kamu kurum ve kuruluşları ile yetkili kamu görevlileri, sigorta şirketleri, araç bakım servisleri otonomlaştırılmış araçların elde ettiği verilere erişme, kaydetme, sınıflandırma, değerlendirme ve depolama gibi çeşitli kişisel verileri işleme faaliyeti gerçekleştirebilecektir. Bu kapsamda bu kişiler, kişisel verileri işleme faaliyetinin araç ve amacını belirleyen gerçek veya tüzel kişiler olarak gündeme gelecek, bu kapsamda veri sorumlusu olarak nitelendirilebileceklerdir.